НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

Факультет інформатики та обчислювальної техніки

Кафедра технічної кібернетики

«На правах рукопису»
УДК 004.72

«До захисту допущено»

Завідувач кафедри
_____ І.Р. Пархомей
(підпис)
“___”_____2018 р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 121 «Інженерія програмного забезпечення»

на тему: Модель захисту інформації при передачі даних радіотехнологією

Виконав: студент другого курсу, групи ІТ-74мп
(шифр групи)

Коновал Ярослав Русланович _____
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник професор, д.т.н. Жураковський Б. Ю. _____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

Факультет інформатики та обчислювальної техніки

Кафедра технічної кібернетики

Рівень вищої освіти – другий (магістерський)
Спеціальність 121 «Інженерія програмного забезпечення»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____І.Р. Пархомей
(підпис)
«___»_____2018 р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Коновалу Ярославу Руслановичу
(прізвище, ім'я, по батькові)

1. Тема дисертації «Модель захисту інформації при передачі даних радіотехнологією»,

науковий керівник дисертації професор, д.т.н. Жураковський Б. Ю.,_____
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «07» листопада 2018 р. №4112-с
2. Термін подання студентом дисертації _____
3. Об'єкт дослідження – Процес захисту інформації в бездротових мережах.
4. Предмет дослідження – Модель захисту даних при передачі даних бездротовою мережою.
5. Перелік завдань, які потрібно розробити – проведення аналізу безпеки бездротових мереж, виділення методів їх захисту та створення моделі захисту бездротових мереж.
6. Орієнтовний перелік ілюстративного матеріалу – п'ять плакатів
7. Орієнтовний перелік публікацій – одна публікація

8. Консультанти розділів дисертації

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

9. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Аналіз предметної області	14.09.2018 р.	
2	Постановка задачі	16.09.2018 р.	
3	Аналіз інформаційного забезпечення	21.09.2018 р.	
5	Аналіз алгоритмічного забезпечення	26.09.2018 р.	
6	Розробка алгоритмічного забезпечення	13.10.2018 р.	
7	Розробка програмного забезпечення	01.11.2018 р.	
8	Маркетинговий аналіз стартап-проекту	11.11.2018 р.	
9	Висновки	15.11.2018 р.	

Студент _____ Коновал Я. Р.
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ Жураковський Б. Ю.
(підпис) (ініціали, прізвище)

АНОТАЦІЯ

Дана магістерська робота присвячена вирішенню задачі захисту інформації в радіоканалах, шляхом застосування комплексних заходів для захисту від можливих атак спрямованих на перехоплення і підміну переданих даних.

Метою магістерської дисертації є проведення аналізу безпеки бездротових мереж, виділення методів їх захисту та створення моделі захисту бездротових мереж.

Для того, щоб досягнути поставленої мети, виконано наступний перелік завдань:

1. Проаналізовано існуючі рішення у галузі захисту інформації через радіомережі
2. Зроблено опис запропонованої розробленої моделі
3. Описано алгоритми, експерименти, досліди даної моделі
4. Виконаний власний стартап проект

Методи дослідження - описовий, методи аналізу та синтезу, експериментальний метод, метод узагальнення.

Наукова новизна даної розробки полягає в тому, що розроблено засіб захисту інформації через радіомережі, застосування якого має значне підвищення рівня безпеки інформації в радіоканалі.

Практична цінність даної розробки в тому, що отримані теоретично і практично результати рекомендуються до впровадження в організаціях, що використовують радіоканал для передачі конфіденційної інформації з підвищеним вимогам до безпеки.

Розмір пояснювальної записки – 114 аркушів, містить 11 ілюстрацій, 27 таблиць, 5 додатків.

ABSTRACT

This master's work is devoted to solving the problem of information security in the radio channels of mobile robotic complexes, through the use of comprehensive measures to protect against possible attacks aimed at intercepting and substituting data transmitted.

The purpose of the master's thesis is to carry out an analysis of the safety of wireless networks, the allocation of methods for their protection and the creation of a model for the protection of wireless networks.

In order to achieve the goal, you need to complete the following list of tasks:

1. Review the existing solutions in the field of information security through the radio network
2. Make a description of the proposed model
3. Describe algorithms, experiments, experiments of this model
4. Make your own startup project

Methods of research - descriptive, methods of analysis and synthesis, experimental method, generalization method.

The scientific novelty of this development lies in the fact that a means of protecting information through the radio network has been developed, the application of which has a significant increase in the level of information security in the radio channel.

The practical value of this development is that the results obtained theoretically and practically are recommended for implementation in organizations that use the radio channel for the transmission of confidential information with increased security requirements.

Explanatory note size – 114 pages, contains 11 illustrations, 27 tables, 5 applications.

Пояснювальна записка
до магістерської дисертації

на тему: МОДЕЛЬ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ПЕРЕДАЧІ ДАНИХ РАДІОТЕХНОЛОГІЄЮ

Київ – 2018 року

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AP (Access Point) – точка доступу в безпровідну мережу

SSID (Service Set Identifier) – ідентифікатор безпровідної мережі

SSL (Secure Socket Layers) – протокол передачі шифрованих даних

WEP (Wired Equivalent Privacy) – протокол захисту даних при передачі по радіоканалу

АІС – автоматизована ідентифікаційна система

КЗЗІ – комплекс засобів захисту інформації

МРК – мобільний робототехнічний комплекс

ОС – операційна система

СЗІ – система захисту інформації

НСД – несанкціонований доступ

ЕОМ – електронно обчислювательна машина

IV (Initialization Vector) – вектор ініціалізації

ВСТУП

В даний час, як в Україні, так і за кордоном ведуться активні роботи зі створення мобільних робототехнічних комплексів (МРК). Сфера застосування таких комплексів є обширною, першочерговими є завдання, у ході яких мобільний робот діє в умовах, небезпечних для знаходження людини. Перспективним є використання автоматизованих робототехнічних комплексів в умовах, коли є загроза життю оператора. У складі пошукової групи МРК можуть здійснювати функції дистанційної розвідки, діючи автономно і передаючи дані по бездротовому каналу.

Науковці створюють пристрої, призначені для виконання різноманітних завдань, в тому числі – для використання виключно в екстремальних умовах. Зазвичай до складу комплексу входить мобільний робот, який має на борту спеціальне обладнання, і система управління, яка, серед інших пристроїв, що включає пультову ЕОМ, встановлену на посту управління робочому місці оператора, а також бортову ЕОМ, встановлену на борту мобільного робота. Зв'язок здійснюється за допомогою бездротового каналу.

Одним з найважливіших завдань є забезпечення необхідної умови захищеності інформації. Найбільш вразливими є дані, що передаються через радіоканал. Від поста управління на бортову ЕОМ передаються команди управління, від бортової ЕОМ на пультову ЕОМ повертаються дані за статусом систем мобільного комплексу та інформація від датчиків (відео камери, радар, приповерхневих сканер тощо). Команди, що передаються роботу по бездротовому каналу, можуть бути перехоплені і модифіковані. Дані, що передаються від мобільного робота на пункт управління, так само можуть бути перехоплені і модифіковані.

До системи аутентифікації в бездротовій мережі пред'являються підвищені вимоги з безпеки. Необхідно використовувати криптографічно стійкі алгоритми, що дозволяють здійснити взаємну аутентифікацію сторін. Окремим важливим

завданням є локалізація активної станції - порушника в межах захищеної бездротової мережі. Необхідно розробити технологію, що дозволяє здійснювати ефективний пошук неавторизованої станції.

Дана магістерська робота присвячена вирішенню задачі захисту інформації в радіоканалах мобільних робототехнічних комплексів, шляхом застосування комплексних заходів для захисту від можливих атак спрямованих на перехоплення і підміну переданих даних.

РОЗДІЛ 1. ОГЛЯД ІСНУЮЧИХ РІШЕНЬ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ПЕРЕДАЧІ ДАНИХ РАДІОТЕХНОЛОГІЄЮ

1.1. ПРОБЛЕМИ ЗАХИСТУ ІНОРМАЦІЇ

Загрозу ототожнюють зазвичай або з характером (видом, способом) дестабілізуючого впливу на інформацію, або з наслідками (результатами такого впливу. Однак такого роду терміни можуть мати багато трактувань. Можливий і інший підхід до визначення загрози безпеки інформації, що базується на понятті "загроза".

Інакше кажучи, поняття загроза жорстко пов'язано з юридичною категорією «шкоду», яку Цивільний Кодекс визначає як «фактичні витрати, понесені суб'єктом у результаті порушення його прав (наприклад, раз угоди або використання порушником конфіденційної інформації), втрати або пошкодження майна, а також витрати, які він повинен буде зробити для відновлення порушеного права і вартості пошкодженного або втраченого майна».

Аналіз негативних наслідків реалізації загроз передбачає ідентифікацію можливих джерел загроз, вразливостей, спосібів їх прояву і методів реалізації. І тоді ланцюжок виростає в схему, представлену на рис. 1.1.

Загрози класифікуються по можливості нанесення шкоди суб'єкту відносин при порушенні цілей безпеки. Збиток може бути заподіяний будь-яким суб'єктом (злочин, вина або недбалість), а також стати наслідком, що не залежить від суб'єкта проявів. Погроз не так вже й багато. При забезпеченні конфіденційності інформації це може бути розкрадання (копіювання) інформації та засобів її обробки, а також її втрата (неумисна втрата, витік).

Рисунок 1.1. Модель реалізації загроз інформаційній безпеці

При забезпеченні цілісності інформації список загроз такий: модифікація (спотворення) інформації; заперечення справжності інформації; нав'язування неправдивої інформації. При забезпеченні доступності інформації можливе її блокування, або знищення самої інформації і засобів її обробки.

Всі джерела загроз можна розділити на класи, обумовлені типом носія, а класи на групи по місцю розташування.

Уразливості також можна розділити на класи за належністю до джерела вразливостей, а класи на групи і підгрупи за проявами. Методи реалізації можна розділити на групи за способами реалізації. При цьому необхідно враховувати, що

саме поняття «метод», застосовне тільки при розгляді реалізації загроз антропогенними джерелами.

Для техногенних і стихійних джерел це поняття трансформується в поняття "передумова".

Структура класифікацій:

а) «Джерела загроз»;

б) «Уразливості»;

в) «Методи реалізації»

Класифікація можливостей реалізації загроз (атак), являє собою сукупність можливих варіантів дій джерела загроз визначеними методами реалізації з використанням вразливостей, які призводять до реалізації цілей атаки. Мета атаки може не збігатися з метою реалізації загроз і може бути спрямована на отримання проміжного результата, необхідного для досягнення надалі реалізації загрози. У разі такої розбіжності атака розглядається як етап підготовки до здійснення дій, спрямованих на реалізацію загрози, тобто як "подготовка до вчинення" протиправної дії. Результатом атаки є наслідки, які є реалізацією загрози та / або сприяють такій реалізації.

Сам підхід до аналізу та оцінки стану безпеки інформації ґрунтується на обчисленні вагових коефіцієнтів небезпеки для джерел загроз і вразливостей, порівняння цих коефіцієнтів з наперед заданим критерієм і послідовному скороченні (виключення) повного переліку можливих джерел загроз і вразливостей до мінімально актуального для конкретного об'єкта.

Вихідними даними для проведення оцінки та аналізу служать результати анкетування суб'єктів відносин, спрямовані на з'ясування спрямованості їх діяльності, передбачуваних пріоритетів цілей безпеки, завдань, розв'язуваних автоматизованою системою та умов розташування та експлуатації об'єкта.

Завдяки такому підходу можливо:

- встановити пріоритети цілей безпеки для суб'єкта відносин;

- визначити перелік актуальних джерел загроз;
- визначити перелік актуальних вразливостей;
- оцінити взаємозв'язок загроз, джерел загроз і вразливостей;
- визначити перелік можливих атак на об'єкт;
- описати можливі наслідки реалізації загроз.

Джерела загроз безпеці інформації поділяються на зовнішні і внутрішні.

До зовнішніх джерел відносяться:

- недружня політика іноземних держав у сфері інформаційного моніторингу, поширення інформації та нових інформаційних технологій;

- діяльність іноземних розвідувальних і спеціальних, направленна проти інтересів України;

- діяльність іноземних економічних структур, спрямована проти інтересів України;

- злочинні дії міжнародних груп, формувань та окремих осіб;

- стихійні лиха і катастрофи.

Внутрішніми джерелами є:

- протизаконна діяльність політичних, економічних і кримінальних структур та окремих осіб в області формування, поширення і використання інформації, спрямована в т. ч. і на нанесення економічної шкоди державі;

- неправомірні дії різних структур і відомств, що призводять до порушення законних прав працівників в інформаційній сфері;

- порушення встановлених регламентів збору, обробки та передачі інформації;

- навмисні дії та ненавмисні помилки персоналу автоматизованих систем, що призводять до витоку, знищення, спотворення, підробки, блокування, затримки, несанкціонованого копіювання інформації;

- відмови технічних засобів і збої програмного забезпечення в інформаційних і телекомунікаційних системах;

- канали побічних електромагнітних випромінювань і наведень технічних засобів обробки інформації.

Способи впливу загроз на об'єкти захисту інформації підрозділяються на інформаційні, апаратно-програмні, фізичні, радіоелек-тронні та організаційно-правові.

До інформаційних способів відносяться:

- порушення адресності та своєчасності інформаційного обміну;

- несанкціонований доступ до інформаційних ресурсів;

- незаконне копіювання даних в інформаційних системах;

- розкрадання інформації з банків і баз даних;

- порушення технології обробки інформації.

Апаратно-програмні способи включають:

- впровадження комп'ютерних вірусів;

- встановлення програмних і апаратних закладних пристроїв;

- знищення або модифікацію даних в інформаційних системах.

Фізичні способи включають:

- знищення або руйнування засобів обробки інформації та зв'язку;

- знищення, руйнування або розкрадання машинних або інших ориги-налів носіїв інформації;

- розкрадання апаратних або програмних ключів і засобів криптогра-фічного захисту інформації;

- вплив на персонал;

- поставку "заражених" компонентів інформаційних систем.

Радіоелектронними способами є:

- перехоплення інформації в технічних каналах її витоку;

- впровадження електронних пристроїв перехоплення інформації в технічні засоби передачі інформації та приміщення;

- перехоплення, дешифрування і впровадження неправдивої інформації в мережах передачі даних і лініях зв'язку;

- вплив на парольно-ключові системи;

- радіоелектронне придушення ліній зв'язку і систем управління.

Організаційно-правові способи включають:

- закупівлі недосконалих або застарілих інформаційних технологій і комп'ютерних засобів;

- невиконання вимог законодавства України в інформаційній сфері;

- неправомірне обмеження доступу до документів, що містять важливу для громадян та органів інформацію.

Таким чином, надійний захист телекомунікаційних мереж від особистого виду загроз можлива тільки на основі побудови комплексної системи безпеки інформації на всіх етапах розробки, введення в дію, модернізації апаратно-програмних засобів телекомунікацій, а також при обробці, зберіганні і передачі по каналах зв'язку інформації з широким застосуванням сучасних засобів криптографічного захисту інформації, яка б включала в себе взаємопов'язані заходи різних рівнів: нормативно-правового; організаційного (адміністративного); програмно-апаратного; технічного.

1.2. ОГЛЯД ІСНУЮЧИХ РІШЕНЬ

Для огляду існуючих рішень захисту інформації при передачі даних радіотехнологією, зазначимо, що в останні роки у зв’язку з безперервним зростанням кількості завдань, пов’язаних із взаємодією між територіально віддаленими об’єктами і відповідно необхідністю передачі по каналах зв’язку конфіденційної інформації, вельми актуальною стає проблема забезпечення безпеки цієї інформації. Розробка моделей і методів забезпечення безпеки інформації, що передається по каналах різної фізичної природи і відповідно з допомогою різних технічних засобів, являє собою важливу задачу.

Для вирішення проблеми забезпечення безпеки інформації, що передається по каналах зв’язку, ще в кінці минулого століття був запропонований спосіб передачі цієї інформації в суміші з цифровим шумом [12, с. 23], що забезпечує приховування переданої зашифрованою або незашифроване від потенційних зловмисників каналів зв’язку. Була розроблена і досліджена комп’ютерна модель, що реалізує запропонований спосіб передачі, яка продемонструвала досить високу надійність виділення корисної інформації з суміші її з цифровим шумом на приймальному кінці каналу зв’язку. Ще кілька років тому були з’ясовані і сформульовані [6, с. 10] завдання, які необхідно опрацювати для реалізації подібних моделей в реальних системах, рекомендовані і методи, що дозволяють звести ймовірність виділення «зломщика» каналів зв’язку інформації з її суміші з цифровим шумом практично до нуля. До зазначених завдань відноситься вирішення проблем початку і закінчення передачі і прийому корисної інформації.

Методи захисту інформації в каналі зв'язку можна розділити на дві групи:

- методи, засновані на обмеженні фізичного доступу до лінії і апаратури зв'язку

- методи, засновані на перетворенні сигналів в лінії до форми, що виключає (ускладнює) для зловмисника сприйняття або спотворення змісту передачі.

Методи першої групи в розглянутому варіанті побудови захищеного зв'язку мають дуже обмежене застосування, так як на основному протязі лінія зв'язку знаходиться поза ведення суб'єкта, організуючого захист. У той же час, по відношенню до апаратури терміналу і окремих ділянок абонентської лінії застосування відповідних заходів необхідно.

Обмеження фізичного доступу передбачає виключення (утруднення):

- безпосереднього підключення апаратури зловмисника до електричних ланцюгів апаратури абонентського терміналу;

- використання для перехоплення інформації електромагнітних полів в навколишньому просторі і наведень у відхідних ланцюгах, мережі живлення і заземлення;

- отримання зловмисником допоміжної інформації про використовуване обладнання і організації зв'язку, що полегшує подальше несанкціоноване втручання в канал зв'язку.

Методи перетворення мовного сигналу, що перешкоджає перехопленню інформації:

-аналоговий

-А. Частотні перетворення

-А1.Інверсія спектру

-А2.Перестановка смуг

- А2.1.Статична перестановка

- А2.2.Змінна перестановка під управлінням криптоболоков

-Б. Часові перетворення

-Б1.Тимчасова інверсія

-Б2.Перестановка відрізків

- Б2.1.Статична перестановка

- Б2.2.Змінна перестановка під управлінням криптоблока

-цифровий:

-В. Перетворення в код з подальшим шифруванням:

-В1.Кодування звуку зі швидкістю 32-64Кб / сек.

-В2.Кодування голосу зі швидкістю 1,2-4,8 Кб/сек.

АБ-Комбіновані мозаїчні перетворення = зв'язок А1 і Б1, зв'язок А2.2. і АБ, Б2.2. і АБ

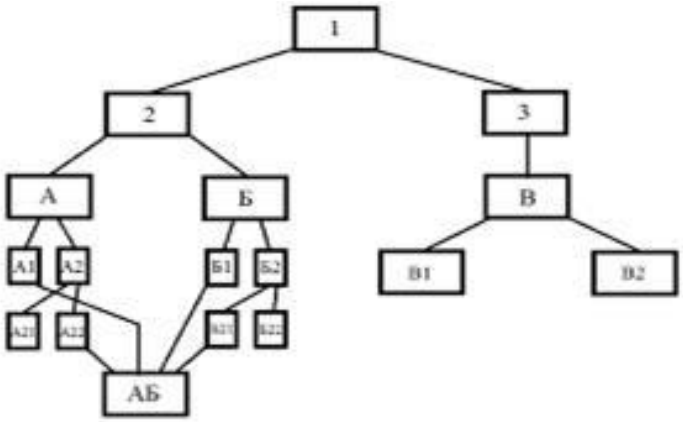


Рисунок 1.2. Комбіновані мозаїчні перетворення

Для захисту інформації, що передається по функціональних каналах зв'язку найбільш ефективним є застосування інформаційних методів приховування інформації, а саме шифрування. Слід зазначити, що для захисту інформації, що передається по радіоканалу, з технічних методів захисту саме інформаційні будуть єдино прийнятними. Це пояснюється тим, що носій інформації (електромагнітна хвиля) не має чітких меж в просторі і локалізувати її будь-якими технічними засобами неможливо.

Для захисту інформації, що передається по дротових лініях зв'язку можливо застосувати методи енергетичного приховування. Це можливо через те, що провідник має чіткі межі в просторі. Для захисту від безконтактного знімання з пасивних способів застосовують екранування кабелів із заземленням екрану, з активних – лінійне зашумлення.

Для захисту від витоку інформації по електричному каналу пасивних способів застосовують фільтрацію, обмеження небезпечних сигналів, захисне відключення, а також екранування ліній, що виходять за межі контрольованої зони з заземленням екрануючої оболонки. На відміну від захисту проводового функціонального каналу зв'язку, в цьому випадку екрануються ділянки провідника, проходять поряд з технічними засобами та іншими провідниками, що несуть інформацію обмеженого доступу, з метою виключення взаємного впливу і наведення в провіднику, що виходить за межі контрольованої зони інформаційного сигналу.

На початку необхідно пояснити сутність зазначених завдань та методів вдосконалення систем зв’язку з передачею корисної інформації в суміші з цифровим шумом, наводиться варіант вирішення проблеми вибору моментів початку передачі інформації і її закінчення; пропонується варіант системи зв’язку з практично нульовою ймовірністю вилучення зломщиком каналу зв’язку кодів переданої інформації з послідовності кодів цифрового шуму.

На сьогоднішній день великий розвиток в області передачі даних отримали бездротові мережі – мережі радіозв’язку. Це пояснюється зручністю їх використання, дешевизною і прийнятною пропускною здатністю. Виходячи з поточної динаміки розвитку, можна зробити висновок про те, що за кількістю і поширеністю бездротові мережі незабаром перевершать провідні мережі.

Ця динаміка безпосереднім чином впливає на вимоги до захисту інформації в бездротових мережах. В даній роботі детально розглядається поточний стан ряду протоколів бездротового зв’язку, дається оцінка перспектив їх застосування і пропонуються варіанти перспективних напрямків досліджень по забезпеченню захисту інформації в бездротових мережах.

В технології бездротових мереж основну увагу приділяють питанням забезпечення безпеки, оскільки проблема надійного захисту інформації служить одним з головних стримуючих факторів розвитку бездротових мереж і систем на їх основі.

Радіомережі (бездротові мережі) забезпечують обмін даними між локальними комп'ютерними мережами, коли використання традиційних кабельних технологій ускладнене або недоцільне. Прикладом ефективного використання бездротової технології радіодоступу є забезпечення зв'язку між сегментами локальних мереж при нестачі фінансових коштів, відсутності дозволу на проведення кабельних робіт або відмову телефонної станції в оренду виділеного каналу. У закритих приміщеннях прокладка кабелю може виявитися неможливою при забороні монтажних робіт.

Основою будь-якої бездротової мережі служить її протокол. Як правило, протокол регламентує топологію мережі, маршрутизацію, адресацію, порядок доступу вузлів мережі до каналу передачі даних, формат переданих пакетів, набір керуючих команд для вузлів мережі і систему захисту інформації. Тому в даній роботі особливу увагу приділено короткому опису протоколів.

Опис протоколів. Все різноманіття протоколів бездротової передачі даних можна класифікувати за кількома різними шляхами, вибравши в якості основного один з параметрів, наприклад топологію мережі, швидкість роботи або алгоритми безпеки. Найбільш поширений метод класифікації в технічній літературі виходить з максимального радіусу дії бездротової мережі. Нижче наведено класифікацію розглянутих протоколів за порядком зменшення радіусу.

WWAN (WirelessWideareanetwork) - в основному це мережі стільникового зв'язку, їх радіус дії складає десятки кілометрів. До цих мереж відносяться наступні протоколи: GSM, CDMAone, iDEN, PDC, GPRS і UMTS.

WMAN (WirelessMetropolitanAreaNetworks - це бездротові мережі масштабу міста. Радіус дії таких мереж декілька кілометрів. Прикладом протоколу цієї мережі служить WiMAX.

WLAN (WirelessLocalAreaNetwork; WLAN) - це бездротова локальна обчислювальна мережа. Радіус дії цього класу мереж — кілька сотень метрів. До них відносяться наступні протоколи: UWB, ZigBee, Wi-Fi.

WPAN застосовуються для зв’язку різних пристроїв, включаючи комп’ютери, побутові прилади та оргтехніку, засоби зв’язку і т. д. Радіус дії WPAN становить від кількох метрів до декількох десятків метрів. WPAN використовується як для об’єднання окремих пристроїв між собою, так і для зв’язку їх з мережами більш високого рівня. Прикладом таких мереж можуть служити протоколи RuBee, X10, Insteon, Bluetooth, Z-Wave, ANT, RFID.

Нижче коротко описується кожен з розглянутих протоколів. Ці протоколи обрані для аналізу внаслідок їх широкого поширення в сучасних бездротових мережах зв’язку. Такий вибір дозволяє дати огляд поточного стану інформаційної безпеки в мережах бездротового зв’язку незалежно від розв’язуваних бездротовими мережами завдань.

Модель OSI. Крім радіусу дії мереж роль протоколів важлива при визначенні рівнів в моделі OSI. Еталонна модель OSI, іноді звана стеком OSI, передбачає 7-рівневу мережеву ієрархію, розроблену Міжнародною організацією за стандартами (International StandardizationOrganization-ISO). Нижче представлено поділ рівнів і вирішувані на цих рівнях завдання.

Група протоколів IEEE 802.X містить опис мережевих специфікацій і дає стандарти, рекомендації та інформаційні документи для мереж і телекомунікацій.

Рекомендації IEEE пов'язані головним чином з двома нижніми рівнями моделі OE1 — фізичним і канальним. Ці рекомендації ділять канальний рівень на два підрівні: нижній-MAC (управління доступом до середовища) і верхній-ЄЕС (управління логічним каналом).

Bluetooth. Протокол передачі інформації по бездротовому каналу зв'язку Bluetooth був розроблений групою компаній Ericsson, IBM, Intel, Toshiba і Nokia. Група розробки була створена на початку 1998 року. 20 травня 1998 року відбулося офіційне представлення спеціалізованої робочої групи (SIG-SpecialInterestGroup), покликаної забезпечити безперешкодне впровадження технології, що отримала назву Bluetooth.

Bluetooth забезпечує обмін інформацією між такими пристроями як кишенькові і звичайні персоналвные комп'ютери, мобільні телефони, ноутбуки, принтери, цифрові фотоапарати, мишки, клавіатури, джойстики, навушники, гарнітури на надійній, недорогій, повсюдно доступній радіочастоті для ближнього зв'язку. Зв'язок цих пристроїв може здійснюватися в радіусі від 10 до 100 метрів один від одного навіть в різних приміщеннях.

UWB. Протокол UWB був розроблений альянсом компаній WiMedia, а в 2007 році цей протокол був затверджений в якості міжнародного стандарту ISO/IEC 26907.

WiMedia UWB є стандартом широкосмугового бездротового зв'язку на коротких відстанях. Протокол зачіпає аспекти взаємодії між пристроями на фізичному рівні (PHY) і підрівні доступу до середовища (MAC). Максимальна швидкість передачі даних між пристроями WiMedia UWB становить 480 Мбіт/с (як і у проводового USB), пристрої працюють в діапазоні частот від 3,1 до 10,6 ГГц. Протокол UWB конкурує з протоколом Bluetooth.

ZigBee. Протокол ZigBee — це стандарт для недорогих, малопотужних бездротових мереж з комірчастою топологією. Низька вартість дозволяє широко застосовувати дану технологію для бездротового контролю і спостереження, а завдяки малій потужності сенсори мережі здатні працювати довгий час, використовуючи автономні джерела живлення.

Протокол був розроблений альянсом компаній ZigBee. Цей альянс служить органом, визначальним для ZigBee стандарти високих рівнів; він також публікує профілі додатків, що дозволяє виробникам вихідних комплектуючих випускати сумісні продукти.

Нижні рівні для даного стандарту розроблені IEEE і визначаються стандартами IEEE 802.15.4-2006.

Insteon. Протокол INSTEON розроблений для управління бездротовими пристроями, призначеними для «розумното будинку». У протоколі передбачена

зворотна сумісність з більш старим протоколом X10. Швидкість передачі сигналу керування за новим стандартом набагато вище, передбачаються вбудовані засоби виявлення помилок і повторної передачі сигналу, а для передачі використовується гібридний канал — радіозв'язок і мережу електроживлення. Однак на відміну від X10 специфікації INSTEON захищені патентами і використовуються тільки його розробниками — компанією SmarthomeTechnology.

Z-Wave. Мережа Z-Wave з функціями самоорганізації і самовідновлення в поєднанні з гнучкими інсталяційними процедурами являє собою просте у використанні мережеве рішення. Протокол Z-Wave і чіп високого ступеня інтеграції забезпечує невисоку вартість без компромісу щодо надійності або універсальності.

Реалізується сумісність додатків і пристроїв Z-Wave, випущених різними виробниками.

Z-Wave підтримує повний спектр пристроїв, включаючи пристрої, що живляться від мережі змінного струму, від батарей, пристрій з фіксованим розташуванням і переміщуються пристрою, а також пристрої, що виконують роль мостів з іншими протоколами.

У технології Z-Wave вузли діляться на три типи: контролери (Controllers), маршрутизуючі виконавчі механізми (Routing Slaves) і виконавчі механізми (Slaves). В реальній мережі всі типи пристроїв можуть працювати в будь-якій комбінації.

ANT. Протокол передачі даних ANT був розроблений компанією Dynastream Innovations.

Даний протокол насамперед розрахований на компактні пристрої з автономним живленням (трансивери, що використовують цей протокол, відрізняються винятково малим струмом споживання) для передачі відносно коротких пакетів даних. Протокол передбачає організацію відкритих і приватних бездротових мереж, в тому числі складного типу з динамічною конфігурацією. Він створений на основі технології PAN (Personal Area Network) і підтримує шари 1-4

стека OSI (OpenSystemsInterconnectionnetworkmodel). Типове застосування такого протоколу — бездротові датчики.

Несуча частота по протоколу ANT — 2,4 ГГц, кількість частотних каналів при цьому дорівнює 125 (крок 1 МГц в діапазоні 2400.. .2524 МГц). Швидкість передачі даних по радіоканалу (включаючи протокол) може становити до 1 Мбіт/с.

RuBEE. RuBee (IEEE P1902.1) - протокол двостороннього бездротового зв'язку в місцевій регіональній мережі з використанням довгохвильового діапазону (LW) і пакетів даних не більше 128 байт. Протокол RUBee подібний до протоколів серії IEEE 802, також відомим як Wi-Fi (IEEE 802.11), WPAN (IEEE 802.15.4) і Bluetooth (IEEE 802.15.1). RuBeenetworked, працює за принципом точка-точка і є розвитком стандартів RFID. RuBee передбачає роботу на низькочастотній несучій (131 кГц), дозволяючи використовувати вузли мережі з малим споживанням енергії.

RFID. RFID Radio Frequency IDentification. Радіочастотна ідентифікація з'явилася більше тридцяти років тому. У 1973 році МаріоКардулло і його співавтори опублікували патент US 3713148, що описує перший пасивний транспондер RFID (радиометку). Розвиток і широке впровадження радіочастотної ідентифікації довго стримувалося відсутністю стандартизації. Але в 90-х роках минулого століття Міжнародна Організація Стандартизації (ISO) прийняла ряд стандартів в області RFID (серія стандартів ISO 18000-6).4.9. X10

XI0 - це міжнародний відкритий індустріальний стандарт, що застосовується для зв'язку електронних пристроїв в системах домашньої автоматизації. Стандарт X10 виділяє методи і протокол передачі сигналів управління електронними модулями, до яких підключені побутові прилади, з використанням звичайної електропроводки або бездротових каналів.

Стандарт X10 розроблений в 1975 році компанією PicoElectronics (Шотландія) для управління домашніми електроприладами. Вважається, що це перший стандарт для домашньої автоматизації.

WI-FI. Wi-Fi створений в 1991 році NCR Corporation/AT&T (згодом — Lucent Technologies і AgereSystems) в Нідерландах. Wireless Fidelity — «бездротова точність» — торгова марка Wi-Fi Alliance для бездротових мереж на базі стандарту IEEE 802.11.

Зазвичай схема Wi-Fi мережі містить не менше однієї точки доступу (так званий режим infrastructure) і не менше одного клієнта. Також можливе підключення двох клієнтів в режимі точка-точка, коли точка доступу не використовується, а клієнти з'єднуються за допомогою мережевих адаптерів «безпосередньо». Точка доступу передає свій ідентифікатор мережі (SSID) за допомогою спеціальних сигналів пакетів на швидкості 0.1 Мбіт/с кожні 100 мс. Тому 0.1 Мбіт/с - це найменша швидкость передачі даних для Wi-Fi. Знаючи SSID-мережі, клієнт може з'ясувати, чи можливе підключення до даної точки доступу. При попаданні в зону дії двох точок доступу з ідентичними SSID приймач може выбирати між ними на основі даних про рівень сигналу.

PDC. PDC (Personal Digital Cellular) — стандарт стільникового зв'язку покоління 2G. Розроблено асоціацією ARIB (Association of Radio Industriesand Business) у квітні 2001 року. Исполвзуетсяисключителвно на території Японії. В даний час кількість абонентів стільникового зв'язку, що працюють на даному стандарті, сократилосв до 10 мільйонів чоловік. Притому, що в період максимальної поширеності цього стандарту кількість абонентів сягала 80 мільйонів чоловік. PDC використовують частотні канали по 25 кГц з модуляцією pi/4-DQPSK з трьома тимчасовими слотами, які забезпечують передачу зі швидкістю 11.2 кбіт/с або 6 тимчасовими слотами зі швидкістю передачі 5.6 кбіт/с.

PDC використовує два діапазони частот 800 МГц і 1,5 ГГц.

IDEN. IDEN (IntegratedDigitalEnhancedNetworks) - технологія для мереж транкінгового і стільникового зв'язку, розроблена компанією MOTOROLA в 1994 році. В основі технології iDEN архітектура GSM, при передачі використовують частотні канали по 25 кГц, при цьому для передачі даних використовується частина

каналу шириною 20 кГц, решта преназначено для захисту каналу. Протокол набув широкого поширення в усьому світі. Діапазон частот - 821-825 МГц.

CDMAOne. Стандарт CDMAOne розроблений в 1995 році як технологічний стандарт групи ANSI. CDMAOne заснований на використанні CDMA (множинного доступу з кодовим поділом).

При побудові системи мобільного зв'язку на основі технології CDMA2000 IX перша фаза забезпечує передачу даних зі швидкістю до 153 кбіт/с, що дозволяє надавати послуги голосового зв'язку, передачу коротких повідомлень, роботу з електронною поштою, Інтернетом, базами даних, передачу даних і нерухомих зображень.

WIMAX. WiMAX (WorldwideInteroperabilityforMicrowave Access) — телекомунікаційна технологія, розроблена з метою надання універсального бездротового зв'язку на великих відстанях для широкого спектру пристроїв (від робочих станцій і портативних комп'ютерів до мобільних телефонів). Заснована на стандарті IEEE 802.16, який також називають Wireless MAN.

Назва «WiMAX» було запропоновано WiMAXForum — організацією, заснованої в червні 2001 року для просування і розвитку технології WiMAX. Форум описує WiMAX як «засновану на стандарті технологію, що надає високошвидкісний бездротовий доступ до мережі, альтернативний виділеним лініям і DSL» Максимальна швидкість — до 1 Гбіт/с.

GSM. GSM (від назви групи GroupeSpecialMobile, пізніше перейменований в Global System for Mobile Communications) — глобальний цифровий стандарт для мобільного стільникового зв'язку з поділом частотного каналу за принципом TDMA і середнім ступенем безпеки. Розроблено під егідою Європейського інституту стандартизації електрозв'язку (ETSI) в кінці 1980-х років.

Комерційне використання стандарту почалося в середині 1991 р., а до 1993 р. було організовано 36 мереж GSM в 22 країнах. На додаток до європейських держав стандарт GSM вибрали багато країн Південної Африки, Близького і Далекого

Сходу, а також Австралія. До початку 1994 р. число абонентів GSM досягло 1.3 мільйона. Термін GSM є скороченням від Global System for Mobile telecommunications — глобальна система мобільних телекомунікацій.

GSM відноситься до мереж другого покоління (Generation 2), хоча на 2017 рік умовно знаходився у фазі 2,75 G завдяки численним розширенням (1G — аналоговий стільниковий зв'язок 2G — цифровий стільниковий зв'язок, 3G — широкосмуговий цифровий стільниковий зв'язок, комутована багатоцільовими комп'ютерними мережами, включаючи Інтернет). 4G - стандарт четвертого покоління мобільного радіозв'язку, відрізняється швидкістю передачі даних, яка перевищує показники 3G в 200-500 разів. 5G (5-е покоління мобільних мереж або 5-го покоління бездротових систем) — назва, яку використовують в деяких наукових працях і проектах для позначення наступних телекомунікаційних стандартів для мобільних мереж після стандартів 4G/IMT-Advanced. Станом на початок 2018 року дана технологія не була повністю визначена у міжнародних стандартах, а лише перебувала у стані розробки. Першим стандартом цієї технології став ухвалений наприкінці 2017 року стандарт New Radio (NR).

GPRS. GPRS (General Packet Radio Service) — пакетна радіозв'язок загального користування) — надбудова над технологією мобільного зв'язку GSM, що здійснює пакетну передачу даних. GPRS дозволяє користувачеві мережі стільникового зв'язку проводити обмін даними з іншими пристроями в мережі GSM і з зовнішніми мережами, включаючи інтернет.

Передача даних розділяється за напрямками «вниз» (downlink, DL) - від мережі до абонента і «вгору» (uplink, UL) - від абонента до мережі. Мобільні термінали поділяються на класи за кількістю одночасно використовуваних таймслотів для передачі і прийому даних.

UMTS. MTS (Universal Mobile Telecommunications System — Універсальна Мобільна Телекомунікаційна Система) — технологія стільникового зв'язку розроблена Європейським Інститутом Стандартів Телекомунікацій (ETSI) для

впровадження 3G в Європі. Як спосіб передачі даних через повітряний простір використовується технологія W-CDMA, стандартизована відповідно до проекту 3GPP в якості відповіді європейських вчених і виробників на вимогу IMT-2000, опубліковане Міжнародним союзом електрозв'язку як набір мінімальних критеріїв для мережі стільникового зв'язку третього покоління.

Згідно специфікаціям стандарту UMTS використовує спектри частот: 1885 2025 МГц для передачі даних в режимі «від мобільного терміналу до базової станції» і 2110 2200 МГц для передачі даних в режимі «від станції до терміналу». В США але через зайнятість спектру частот в діапазоні 1900 МГц GSM виділені діапазони 1710 1755 МГц і 2110 2155 МГц відповідно. Крім того, оператори деяких країн (наприклад, американський AT&T Mobility) додатково експлуатують смуги частот 850 і 1900 МГц. Уряд Фінляндії на законодавчому рівні підтримує розвиток мережі стандарту UMTS900, що покриває важкодоступні райони країни і використовує діапазон 900 МГц (в даному проекті беруть участь такі компанії, як Nokia і Elisa).

Одним із найпоширеніших підходів до оцінки якості захисту інформації є визначений поділ реалізованих функцій і завдань, експлуатаційних характеристик і вимог у відповідність технічним завданням на створення системи захисту. Інший спосіб, який використовується у вітчизняній та закордонній практиці - це аналіз функціональної надійності системи, яка також характеризує якісний рівень системи інформаційної безпеки (СІБ).

Кількісний рівень захисту автоматизованих інформаційних систем (АІС) характеризується двома основними групами показників:

1. Відносна кількісна оцінка, яка є числом (клас, категорія, нормалізоване значення), що вимагає порівняння з іншими числами, прийнятими як еталон. Для їх визначення використовуються експертні оцінки. Найбільш важливим моментом якісного оцінювання є питання про корекцію та узгодження похибок, які виникають через суб'єктів незалежних оцінок - експертів. Найбільш популярним методом

проведення експертизи є метод Делфі і його модифікації. Експертиза може бути спрямована на оцінку ефективності системи захисту, рівня допустимого ризику, рівня захищеності окремих підсистем і ін.

2. Абсолютна кількісна оцінка захисту інформації в АІС може характеризувати витрати, виражені в грошовому еквіваленті, частоту несприятливих подій або інші показники, які є значущими в частині забезпечення захисту інформації.

Абсолютні кількісні показники можуть бути систематизовані в наступні різновиди:

1.Технічні. У цю групу входять:

- кількість загроз, що розпізнаються, визначає кількість загроз, що можуть розпізнаватися та оброблятися. Загроза вважається розпізнаною, якщо її характеристики збігаються з описами, що знаходяться в системі інформаційної безпеки (СІБ);

- якість протистояння загрозам - визначається здатністю СІБ адекватно реагувати на розпізнані загрози. У реальному житті виникають загрози, на які автоматизованим інформаційним системам (АІС) досить важко реагувати. У такій ситуації бажано відзначити у протоколі ті дії, які здійснюються загрозою;

- зменшення продуктивності АІС у цілому - відображає зменшення продуктивності АІС унаслідок необхідності реалізації дій, передбачених політикою безпеки. Прикладами можуть служити плати шифрування, які зменшують швидкість передачі даних через необхідність шифрувати при передачі і дешифрувати при прийомі даних і т. д. [4].

2. Організаційні. Цей вид показників характеризує кількість додатково залученого персоналу для обслуговування СІБ. При реалізації функцій безпеки залучається додатковий персонал - інженери, програмісти, адміністратори систем, менеджери АІС із безпеки.

3. Економічні. До даного різновиду належать наступні показники:

- вартість створення, впровадження, експлуатації та навчання користувачів і підтримки. До них також належить заробітна плата працівників, котрі виконують специфічні для роботи;

- витрати специфічних матеріалів. Передбачає використання спеціальних витратних матеріалів у роботі. Як приклад можна розглядати додаткові магнітні носії, необхідні для реалізації резервного копіювання;

- витрати на відновлення нормальної роботи після реалізації загрози. У них включаються витрати інформаційних, технічних, трудових і інших ресурсів на відновлення нормальної роботи АІС;

- коефіцієнт зменшення потенційних втрат, що характеризує відношення між показником зменшення втрат і величини можливих втрат.

Також варто зазначити, що під час оцінки проектів у галузі інформаційного бізнесу в загальному і систем інформаційної безпеки АІС, зокрема, неможливо однозначно визначити вартість того чи іншого ресурсу або активу АІС, який може бути втрачений внаслідок реалізації тієї чи іншої загрози. Тому використовуються ймовірнісні моделі, що дозволяють розраховувати економічні показники.

Розглядаючи втрати АІС, необхідно відзначити, що вони можуть бути технічними, організаційними, технологічними, економічними, причому вони випливають одне на одного і втрати одного рівня тягти за собою втрати наступних рівнів. У тієї ж годину, при розробці ефективної системи повинна враховуватись величина виграшу порушника, і зробити так, щоб дана величина мінімізувалася.

Сукупності базових стандартів повинні адаптуватися і конкретизуватися стосовно до певних класів проектів, функцій, процесів і компонентів інформаційних систем. У зв'язку з цією потребою виділилося і сформувалося поняття «профілів» як основного інструменту функціональної стандартизації. Зрозуміло, що число можливих профілів захисту у багато разів перевищує вихідну кількість документів, на яких вони можуть базуватися, тому провести апріорну оцінку ефективності всіх можливих профілів неможливо. З іншого боку, профіль

захисту повинен створюватися або вибиратися, виходячи з вимог до показників інформаційної безпеки, встановлених замовником зазналегідь. Прийняті підходи, включаючи ті з них, які зазначені в існуючих стандартах, не дозволяють зробити такий вибір, надзвичайно важливий для практики. Оцінку ж ефективності профілів захисту можна здійснити тільки з використанням комплексних показників, які мають імовірнісний або вартісний характер. При цьому варто звернути увагу на те, що на відміну від офіційних нормативних документів, в аналітичних матеріалах прямо вказується на необхідність використання як головного критерію ефективності СЗІ відповідної ймовірності.

Імовірнісні методи знайшли широке поширення в практиці забезпечення безпеки та інших прикладних областях. Згідно з цими методами рівні гарантій безпеки СЗІ трансформуються в довірчі ймовірності відповідних оцінок показників [5].

По-перше, оцінка оптимального рівня гарантій безпеки багато в чому залежить від збитку, пов'язаність язаного з помилкою у виборі конкретного значення показника ефективності. По-друге, для отримання чисельних оцінок ризику необхідно знати розподіл низькі випадкових величин. Це певною мірою обмежує кількісне дослідження рівнів гарантій безпеки, що надаються СЗІ, але, тим не менш, у багатьох практичних випадках такі оцінки можна отримати, наприклад, за допомогою імітаційного моделювання або за результатами активного аудиту СЗІ.

Оцінка ефективності захисту повинна обов’язково враховувати як об’єктивні обставини, так і ймовірні фактори.

Питання оцінки ефективності СЗІ від НСД:

1.Оцінка коректності реалізації механізмів захисту СЗІ від НСД. На практиці провести таку оцінку є досить важким завданням. Оскільки можливий варіант, коли встановлена у Вашій інформаційній системі СЗІ від НСД не перехоплює і не аналізує лише один подібний спосіб звернення до файлового об’єкту, і, за великим рахунком, вона стає цілком даремною (рано чи пізно, зловмисник виявить даний

недолік засобів захисту і скористається ним). Звідси отримуємо вимогу до коректності реалізації СЗІ від НСД - вона повинна контролювати доступ до ресурсу за будь-якого способу звернення до ресурсу (ідентифікації ресурсу).

2.Оцінка достатності (повноти) набору механізмів захисту у складі СЗІ від НСД.Тут ситуація багато в чому схожа із ситуацією, описаною вище. Наприклад, вимога до достатності механізмів у СЗІ від НСД для захисту конфіденційних даних у нормативних документах виглядає наступним чином: «Чи повинен здійснюватися контроль доступу суб'єктів до ресурсів, що захищаються відповідно до матриці доступу». Природно виникає неоднозначність визначення того, що віднести до ресурсів, які захищаються? Крім того, необхідно розуміти, що безліч комп'ютерних ресурсів (особливо, коли мова йде про універсальну ОС) для корпоративних додатків зайві, в першу чергу, це стосується всіляких зовнішніх пристроїв.

На думку фахівців, об'єктивним видом оцінки ефективності СЗІ є функціональне тестування, призначене для перевірки фактичної працездатності реалізованих механізмів безпеки та їх відповідності висунутим вимогам, а також гарантування отримання статистичних даних [6]. У силу того, що засобам безпеки властиві обмежені можливості з протидії загрозам, завжди існує імовірність порушення захисту, навіть якщо під час тестування механізми безпеки не були обійдені або блоковані. Для оцінки цієї ймовірності повинні проводитися додаткові дослідження. У методичному плані визначення ефективності СЗІ має полягати у виробленні судження щодо придатності способу дій персоналу або пристосованості технічних засобів до досягнення мети захисту інформації на основі вимірювання відповідних показників, наприклад, при функціональному тестуванні.

Ефективність оцінюється для вирішення наступних завдань:

- прийняття рішення про допустимість практичного використання СЗІ в конкретній ситуації;
- виявлення внесків різних факторів у досягнення мети;
- встановлення шляхів підвищення ефективності СЗІ;

- порівняння альтернативних варіантів систем.

Таким чином, при використанні сучасної методичної бази, оцінка ефективності СЗІ носить, в основному, нечіткий, суб'єктивний характер; практично повністю відсутні нормовані кількісні показники, що враховують можливі випадкові чи навмисні дії. У результаті досить складно, а часто і неможливо, оцінити якість функціонування інформаційної системи за наявності несанкціонованих впливів на її елементи, а, відповідно, і визначити, чим один варіант проектованої системи краще іншого. Можливим вирішенням проблеми комплексної оцінки ефективності СЗІ є використання системного підходу, що дозволяє ще на стадії проектування кількісно оцінити рівень безпеки та створити механізм управління ризиками. Але цей шлях реалізується за наявності відповідної системи показників і критеріїв.

Підсумовуючи все сказане раніше, визначимося з вихідними положеннями, необхідними для вибору ефективного рішення:

1. СЗІ від НСД, що належать до одного класу захищеності, можуть бути орієнтовані на вирішення різних завдань захисту інформації та забезпечувати принципово різний рівень захищеності (ефективність).

2. Ефективність СЗІ від НСД визначається тим, наскільки коректно реалізовані в ній механізми захисту і наскільки достатній набір механізмів захисту стосовно ресурсів, що використовуються, та завдань, що вирішуються.

3. Реальну ефективність СЗІ від НСД можуть оцінити лише фахівці, бажано незалежні експерти із числа розробників засобів захисту, які володіють необхідними знаннями з архітектурної організації системних засобів, зокрема сучасних ОС.

Існують наступні методи та засоби оцінки ефективності СЗІ:

1. Метод порівняльного багатовимірного аналізу.

Цей метод створений для визначення ступеня взаєбагато впливу загроз та причин їх виникнення (і як результат - оцінка ефективності системи захисту інформації). Суть методу можна звести до такого узагальненого алгоритму:

- складається перелік об’єктів, що оцінюються, і вибираються ознаки, за якими буде проводитись оцінка. В даному випадку під об’єктами оцінки будемо розуміти показники захищеності обчислювальної системи, а під ознаками - сукупність параметрів, що характеризують ці показники;
- цей перелік слугує основою для формування матриці ознак X(p,w), де p - кількість ознак, а w - кількість об’єктів, що оцінюються. Кожному об’єкту ставиться у відповідність рядок матриці із p ознак.

По отриманій матриці відстаней між показниками здійснюються їх зіставлення між собою, яке дає змогу впорядкувати показники за ступенем важливості, встановити залежності між ними, оцінити ступінь їх взаєбагато впливу.

З використанням цього методу було проведено порівняльний аналіз загроз інформації та причин, які впливають на їх виникнення, кількох комп’ютерних мереж, що експлуатуються в державних установах. Для формування матриці ознак використовувався метод експертного опитування посадових осіб, до компетенції яких входить адміністрування (як технічне, так організаційне) комп’ютерних мереж. Під час такого опитування адміністраторам комп’ютерних мереж пропонувалося заповнити анкету, в якій були перелічені загрози інформації та причини їх виникнення, шляхом визначення пріоритету кожної з них за десятибальною шкалою. Головною вимогою при заповненні анкети було врахування конкретних умов експлуатації комп’ютерної мережі. Обробка результатів опитування відповідно до викладеної вище методики дала змогу оцінити взаємний вплив існуючих загроз і скоригувати відповідним чином політику захисту інформації.

Методи аналізу ризиків інформаційних систем (ІС).

На даний час при побудові СЗІ АС особливого значення набуває завдання побудови моделей загроз інформації. Існує чимало алгоритмів, які здійснюють аналіз ризиків ІС. До найбільш відомих алгоритмів належать CRAMM і RiskWatch. Зазначені алгоритми мають ряд переваг та набули широкого поширення.

Метод CRAMM був розроблений Службою Безпеки Великобританії за завданням Британського уряду і використовується як державний стандарт, починаючи з 1985 р., урядовими і комерційними організаціями Великобританії.

CRAMM припускає поділ усієї процедури на три послідовних етапи. Завданням першого етапу є відповідь на питання: «Чи достатньо для захисту системи застосування засобів базового рівня, що реалізують традиційні функції безпеки, чи необхідно провести більш детальний аналіз?». На другому етапі проводиться ідентифікація ризиків і оцінюється їх величина. На третьому етапі вирішується питання про вибір адекватних контрзаходів.

Методика CRAMM для кожного етапу визначає набір вихідних даних, послідовність заходів, анкети для проведення запитів, списки перевірки і набір звітних документів.

Якщо за результатами проведення першого етапу встановлено, що рівень критичності ресурсів є дуже низьким і існуючі ризики свідомо не перевищать деякого базового рівня, то до системи висувається мінімальний набір вимог безпеки. У цьому випадку велика частина заходів другого етапу не виконується, а здійснюється перехід до третього етапу, на якому генерується стандартний список контрзаходів для забезпечення відповідності базового набору вимог безпеки.

На другому етапі проводиться аналіз загроз безпеки та цілісності. Вихідні дані для оцінки аудитор отримує від уповноважених представників організації в ході відповідних запитів.

На третьому етапі вирішується завдання управління ризиками, що складається у виборі адекватних контрзаходів.

Рішення про впровадження в систему нових механізмів безпеки або про модифікацію діючих приймає керівництво організації. Завданням аудитора є обґрунтування рекомендованих контрзаходів для керівництва організації.

Метод RiskWatch. Програмне забезпечення RiskWatch розробляється американською компанією RiskWatchInc. і є потужним засобом аналізу і управління

ризиками. В сімейство RiskWatch входять програмні продукти для проведення різних видів аудиту безпеки.

У методі RiskWatch як критерії для оцінки та управління ризиками використовуються «прогнозування річних втрат» (ALE) і «повернення від інвестицій» (ROI). Сімейство програмних продуктів RiskWatch має масу переваг.

RiskWatch допомагає провести аналіз ризиків і зробити обґрунтований вибір заходів і засобів захисту. Використовувана в програмі методика включає в себе 3 фази.

Перша фаза - визначення предмету дослідження. На даному етапі описуються параметри організації - тип організації, склад досліджуваної системи. Опис формалізується у ряді підпунктів. Далі кожен з обраних пунктів описується докладно. Для полегшення роботи аналітика в шаблонах даються списки категорій захищених ресурсів, утрат, загроз, уразливих місць і заходів захисту. З них потрібно вибрати ті, що реально присутні в організації.

Друга фаза - введення даних, що описують конкретні характеристики системи. Дані можуть вводитися вручну або імпортуватися зі звітів, створених інструментальними засобами дослідження вразливості комп'ютерних мереж. На цьому етапі докладно описуються ресурси, втрати та класи інцидентів. Класи інцидентів отримуються шляхом зіставлення категорії втрат і категорії ресурсів. Для виявлення можливих уразливостей використовується опитувальник, база якого містить більше 600 питань. Питання пов'язані з категоріями ресурсів. Допускається коректування питань, виключення або додавання нових, встановити частоту виникнення кожної з виділених загроз, ступінь вразливості і цінність ресурсів. Усе це використовується і надалі для розрахунку ефективності впровадження засобів захисту.

Третя фаза - оцінка ризиків. Спочатку встановлюється зв'язок між ресурсами, втратами, загрозами і вразливими місцями, виділеними на попередніх етапах. Для ризику розраховуються математичні очікування втрат за рік:

$$L = P * V, \quad (1)$$

де L - сума втрат від загроз інформації за рік; P - частота виникнення загроз протягом року; V - вартість ресурсу, який під загрозою.

Розглянуті методики дозволяють оцінити чи переоцінити рівень поточного стану інформаційної безпеки АС, розробити концепцію і політику безпеки АС, а також запропонувати плани захисту від виявлених загроз і вразливих місць.

Недоліки розглянутих методів аналізу:

1. Обмежена область застосування. Методика аналізу інформаційних ризиків CRAMM набагато краще підходить для аудиту вже існуючих АС, що знаходяться на стадії експлуатації, ніж для інформаційних систем, що знаходяться на стадії розробки.

2. Нехтування комплексним підходом при аналізі ризиків. Метод RiskWatch робить аналіз ризиків на програмно-технічному рівні захисту, без урахування організаційних та адміністративних чинників. Метод не враховує комплексний підхід до інформаційної безпеки. Крім того, RiskWatch розглядає ризики як математичне очікування втрат. Ця методика не враховує багатьох факторів, які впливають на безпеку інформації.

3. Неможливість розширення бази знань. Сучасні засоби аналізу інформаційних ризиків (наприклад, CRAMM) не передбачають розширення їх бази знань. Відсутність зазначеної можливості викликає суттєві труднощі під час процедури аналізу ризиків конкретної організації.

4. Висока вартість ліцензії. Існуючі засоби для аналізу інформаційних ризиків характеризуються високою вартістю ліцензії.

Крім того, програмне забезпечення CRAMM і RiskWatch існує тільки англійською мовою.

Топології. Всі перераховані бездротові мережі працюють в одному або декількох варіантах топології.

Топологія точка - точка - найпростіший варіант організації мережі з двох пристроїв. Як правило, вузли цієї мережі є рівноправними, тобто мережа однорангова.

Ця топологія характерна для Bluetooth, ANT, RFID, RuBcc, RDC, WI-FI, Insteon, UWB, ZigBcc та інших.

Топологія «Зірка» служить основою організації всіх сучасних мереж зв'язку та обчислювальних мереж. Цю топологію використовують протоколи WI-FI, Insteon, ZigBcc, UWB, IDEN,CDMAOne, WIMAX, GSM, GPRS, U'T. MS.

Топологія «багатоячейковая мережа» - базова повнозв’язна топологія комп'ютерних мереж і мереж зв'язку, в якій кожна робоча станція мережі з'єднується з усіма іншими робочими станціями цієї ж мережі. Характеризується високою відмовостійкістю, складністю налаштування і надмірною витратою кабелю в провідних мережах. Кожен вузол має кілька можливих шляхів з'єднання з іншими вузлами, за рахунок цього така топологія дуже стійка. Так як зникнення одного з каналів не призводить до втрати з'єднання між двома комп'ютерами. Ця топологія допускає з'єднання великої кількості вузлів і характерна, як правило, для великих мереж, вона будується з нолносвязной нутом видалення деяких можливих зв'язків.

Топологія застосовна для мереж з використанням протоколів UWB, WI-FI.

Топологія «кластерне дерево» утворюється в основному у вигляді комбінацій вищеназваних топологій обчислювальних мереж. Підстава дерева обчислювальної мережі розташовується в точці (корінь), в якій збираються комунікаційні лінії інформації (гілки дерева).

Обчислювальні мережі з деревовидною структурою будуються там, де неможливе безпосереднє застосування базових мережевих структур в чистому вигляді.

Методи поділу доступу до радіоканалу. Використання цих методів доступу в сучасних протоколах передачі інформації та бездротових каналах зв'язку викликано

необхідністю передавати великі обсяги інформації за короткий проміжок часу, підтримувати зв'язок з декількома абонентами у вузьких діапазонах частот.

У сучасних протоколах передачі даних передбачається три основні методи поділу доступу пристроїв зв'язку до радіоканалу CDMA, FDMA, TDMA. Також існує ряд їх модифікацій.

CDMA. Code Division Multiple Access (CDMA) це інший метод доступу до каналу, який використовується в мобільній телефонії третього покоління (3G). CDMA є розширенням декількох технологій доступу, який використовує унікальну схему кодування, що дозволяє декільком користувачам одночасно спілкуватися але одному фізичному каналу. Таким чином, кожній групі користувачів надається унікальний загальний код, причому не може бути, щоб в одному й тому ж каналі працювали нееколько користувачів з різними кодами, і спілкуватися і розуміти один одного може єдина група користувачів, які мають один і той же код.

Основна особливість цієї технології в тому, що вона дозволила збільшити кількість сигналів для заданої частотної смуги. Первинний стандарт CDMA, відомий також як IS-95 або edmaOne, до цих нір використовується в мережах мобільного телефонії 2G. CDMA забезпечує більш високу але порівняно з іншими методами доступу швидкість передачі даних.

Щоб продемонструвати відмінності в роботі трьох методів поділу доступу до каналу, припустимо, що в одній кімнаті знаходиться дві групи абонентів. Використовуючи FDMA, члени кожної групи мають різними частотними смугами голосового зв'язку, тобто здійснюється поділ але частоті. В системі TDMA кожній групі відводиться для розх'овора свій часовий інтервал, тобто здійснюється поділ але часу. І, нарешті, CDMA надає обом групам можливість спілкуватися на різних мовах на однакових частотах в один і той же час, тобто реалізується розділення але кодом.

CSMA. Carrier Sense Multiple Access (CSMA) імовірнісний остьовий протокол канального (MAC) рівня. Вузол, що бажає передати пакет даних, виконує

процедуру оцінки чистоти каналу, то мережу протягом заздалегідь заданого часу визначає рівень шуму в передавальної середовищі. Якщо передавальне середовище оцінюється як чисте, вузол може передати пакет даних. В іншому випадку, виконується інша передача, вузол «відсторонюється», то мережа, перш ніж знову почати процедуру відправки пакета, вузол чекає певний час.

На практиці більш поширена модифікація цієї технології CSMA/CD, що передбачає контроль колізій. Існує також технологія CSMA/CA, в якій вживаються заходи але виключення колізій.

Безпека бездротових мереж. Безпека бездротових мереж залежить від використання ряду технологій: шифрування, цифрового підпису, паролів, зміни ключів та іншого. Те, як використовуються ці технології сильно впливає на рівень захищеності мережі. Іноді, методика використання раніше перерахованих технологій така, що вони ніяк не впливають на рівень захищеності мережі. Ці питання детально розглядаються нижче.

Шифрування. Наведено алгоритми шифрування, що застосовуються в кожній з технологій, у переліку вказана технологія, стандарт шифрування і його режим.

Bluetooth-E0-ЄCB;

UWB-ÀES-CBC;

ZigBee-AES-CBC;

Insteon - Rollingcodesystem - потокове;

Z-Wave-3DES тільки в 100 серії-ЄCB;

ANT-ні;

RuBee-AES;

RFID-Cryptol, des-асиметричний;

X10-ні;

WI-FI - RC4, AES-CBC;

PDC-A5-потокове;

IDEN-A5-потокове;

CDMA-CME A-ЄCB;

WIM AX-3DES, AES-ЄCB;

GSM - A5 (COMP-128) - потокове;

GPRS-GEAI, Cl'.A2 - потокове;

UMTS-A5 (COMP-128) KASUMI MILENÀGE-потокове.

Стандарт шифрування E0. У стандарті Bluetooth застосовується потоковий шифр E0, побудований на базі трьох лінійних генераторів зсуву. Ця схема застосовується в Bluetooth в режимах забезпечення безпеки 2 і 3. Дані режимні безпеки застосовуються в протоколі Bluetooth v4.2.

У протоколі Bluetooth v4.2 (і більш ранніх версій, що працюють в режимах безпеки 2 і 3) два встановлюють з'єднання пристрою одночасно отримують однаковий сеансовий ключ у випадку, якщо користувач встановив для них однаковий PIN. Слід зазначити, що якщо PIN-код коротше 16 байтів, то для генерації сеансового ключа як доповнення до значення поточного PIN-коду використовується BD ADDR.

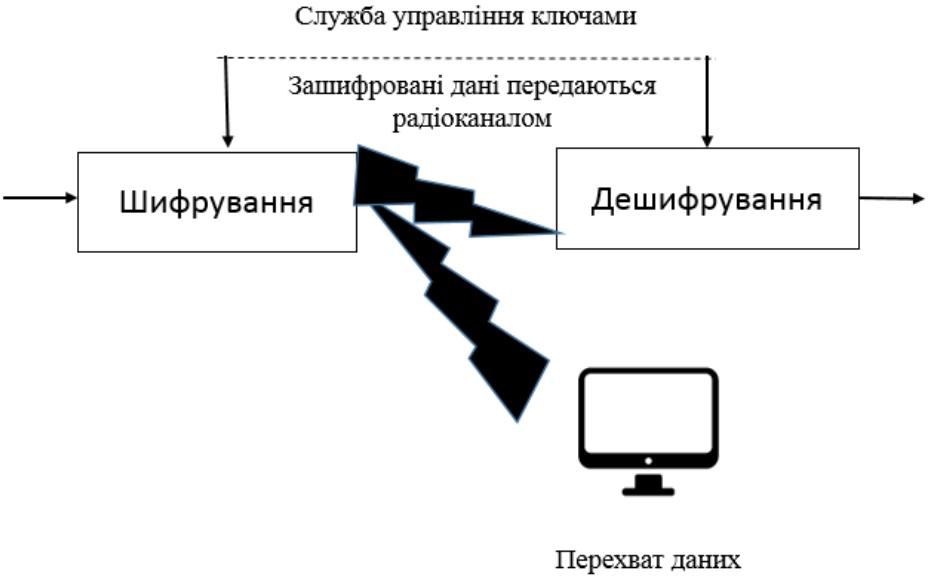


Рисунок 1.3. Перехват даних при шифруванні

Основою процедури шифрування в протоколі Bluetooth служить алгоритм потокового шифрування E0. Ключ потоку підсумовується, але схемі XOR з бітами відкритого тексту і передається на пристрій. Ключ потоку генерується за допомогою криптографічного алгоритму на базі лінійного рекурентного регістра (ЛРР). Функція шифрування отримує такі вхідні дані: головний ідентифікатор (BDADDR). 128-бітне випадкове число (EN_RAND), номер слота і ключ шифрування, який також ініціалізує ЛРР, якщо шифрування включено. Номер слота, який використовується в потоковому шифрі, змінюється з кожним пакетом, змінюючи тим самим ініціалізацію ядра шифру, інші ж неременні при цьому не змінюються.

Ключ шифрування КС генерується з поточного сеансового ключа і може мати довжину від 8 до 128 біт. Встановлення розміру ключа відбувається в ході встановлення сеансу шифрування між пристроями. Початковий розмір ключа вноситься в пристрій виробником, і розмір його не завжди максимальним.

Слід зазначити, що алгоритм E0 не сертифікований FIPS як національний стандарт.

Є теоретична оцінка стійкості даного алгоритму. При атаці зі знанням відкритого тексту потрібно 238 переборів, в той час як при атаці грубої сили необхідно перебрати 2128 можливих ключів.

Шифр Діффі-Хеллмана на еліптичних кривих. У режимі безпеки 4 але протоколу Bluetooth v4.2 використовується пара ключів безпечного простого сполучення (SecureSimplePairing SSP). Ця пара ключів являє собою ключі алгоритму асиметричного шифрування Діффі Холмана на еліптичних кривих.

Даний алгоритм надійний: реалізованих на практиці ефективних атак на EAM алгоритм в даннвій момент не існує. Але є ймовірність того, що атака виявиться успішною при програмній і апаратній реалізації алгоритму.

Стандарт шифрування AES. Даний стандарт шифрування найбільш широко застосовується для захисту бездротових каналів передачі інформації. Він

використовується в протоколах UWB, ZigBee, RuBee, WI-FI і WIMAX. У зв'язку з широким розповсюдженням даного алгоритму його опис в даній роботі нс наводиться. Якщо ключі генеруються на кожен сеанс надійною системою розподілу секрету, ефективних атак на даний алгоритм.

Шифр CMEA. Безпека зв'язку забезпечується також застосуванням процедур аутентифікації та шифрування повідомлень. У CDMA для генерації 128 біт ключа в стільникового зв'язку використовується стандартний алгоритм аутентифікації і шифрування мови CAVE (Cellular Authentication Voice Encryption). Ключ називається SSD (Shared Secret Date «загальні секретні дані»). Ці дані генеруються на основі а-ключа, який зберігається в мобільній станції, з отриманого від мережі псевдовипадкового числа. Загальні секретні дані (SSD) генерує алгоритм CAVE. Вони поділяються на дві частини: SSD-A (64 біта), призначену для вироблення цифрового підпису (authenticationsignature), і SSD-B (64 біта), призначену для генерації ключів, використовуваних для шифрування мови і передачі сигналу повідомлення. SSD може використовуватися постачальниками послуг для місцевої аутентифікації при роумінгу. Нові загальні секретні дані (SSD) можуть генеруватися при переміщенні мобільної станції до чужої мережі або з поверненні до домашньої мережі.

Алгоритм Rolling code system. Цей шифр, названий також KccLoq, використовує лінійний рекуррентнийрсіліетр зсуву. Довжина основного регістру 32 біта, довжина додаткового регістра 5 біт. Шифрування проводиться побитним підсумовуванням е ключем. Для даного алгоритму існують ефективні атаки. Наприклад, щоб отримати систему лінійних рівнянь, що дозволяє відновити початкове заповнення лінійного регістру, досить нутом прослуховування ключової послідовності перехопити її 216 символів.

Алгоритм Crypto 1. Даний алгоритм використовує комбінацію лінійних і нелінійних рекурентних регістрів. Довжина ключа 48 біт.

ВИСНОВКИ ДО РОЗДІЛУ 1

Проагалізовано проблеми захисту інформації та розглянуто модель реалізації загроз інформаційної безпеки. Переглянуто існуючі рішення захисту інформації при передачі даних радіотехнологією.

Розглянуто метод перетворення мовного сигналу, такий як комбіновані мозаїчні перетворення.

Також описано класифікацію протоколів WWAN, WMAN, WLAN, WPAN. Еталона модель OSI.

Проаналізовано протоколи Bluetoooth, UWB, ZigBee, Insteon, Z-Wave, ANT, RuBEE, RFID, X10, Wi-Fi, PDC, IDEN, CDMAone, WIMAX, GSM, GPRS, UMTS.

Розглянуто методи аналізу ризиків інформаційних систем CRAMM, Risk Watch.

Наведено алгоритми шифрування E0, Діффі-Хеллмана, CMEA, Rolling code system, Crypto 1.

РОЗДІЛ 2. АНАЛІЗ МОДЕЛІ

2.1 БЕЗДРОТОВІ МЕРЕЖІ СТАНДАРТУ 802.11

Протокол 802.11 містить ряд вразливостей, пов'язаних зі структурою механізму захисту інформації. Одним з таких слабких місць є протокол WEP, що забезпечує шифрування інформації, використовуючи секретний ключ [17]. Крім того, стандарт 802.11 не регламентує такі важливі питання, як розподіл секретних ключів між станціями мережі і механізм аутентифікації.

Філософія захисту інформації в бездротових мережах багато в чому відрізняється від забезпечення безпеки дротових мереж. Для захисту звичайної провідної мережі від зовнішніх атак досить створити безпечний периметр з мережевих екранів на тих мережевих інтерфейсах, через які здійснюється підключення внутрішньої захищеної мережі до зовнішніх відкритих сегментів. У разі бездротової інфраструктури даного підходу явно недостатньо. При відсутності надійної системи аутентифікації зловмисник може увійти у внутрішню мережу, просто опинившись в зоні з достатнім рівнем сигналу. Навіть при неможливості зареєструватися в мережі атакуюча сторона має потенційну можливість для здійснення перехоплення всього трафіку внутрішньої мережі.

Найбільш поширеною версією стандарту IEEE 802.11 є версія 802.1 lb, забезпечує передачу даних на швидкості до 11 Мбіт/с. Пристрої, що працюють в даному стандарті, використовують кілька каналів в діапазоні частот від 2400 до 2483.5 МГц. Максимальна дальність стійкого зв'язку може досягати 300 м в межах прямої видимості, але при збільшенні відстані можливе істотне зниження швидкості передачі даних.

Стандарт IEEE 802.11 призначений для створення безпечної мережевої архітектури обміну даними між мережевими пристроями за допомогою радіоканалу. Однак з точки зору критеріїв безпеки є серйозні недоліки, ігнорування яких може призвести як до можливих витоків інформації, так і до виходу з ладу всієї

мережевої інфраструктури в разі атаки типу «Відмова в обслуговуванні» [9]. У порівнянні зі звичайною дротовою мережею, доступ до якої може бути обмежений фізичними методами, в разі використання радіоканалу неможливо гарантувати відсутність перехоплення і модифікації переданих даних.

Серед стандартних засобів захисту, передбачених стандартом 802.11, слід особливо виділити протокол WEP.

Історія розвитку бездротових мережевих (WLAN) технологій починається з 1980 року, з відкриттям Американської Федеральної комісії з комунікацій (FCC) частини радіочастот для використання бездротовими мережами. Зростання кількості таких мереж було порівняно невисоким у період з 1980 по 1990. Зараз по всьому світу спостерігається значне збільшення в цьому секторі індустрії та зростаюча зацікавленість з боку споживачів, багато в чому викликана збільшеною смугою пропускання закладеної в стандарті 802.11 b. Основні характеристики бездротових мереж стандарту 802.11 наведені в таблиці 2.1.

Характеристика	Опис
Фізичний рівень	Метод прямої послідовності (Direct Sequence Spread Spectrum), метод частотних стрибків (Frequency Hopping Spread Spectrum), передача в інфрачервоному спектрі (IR)
Частотний діапазон	2,4 ГГц (2,4-2,483 ГГц) і 5ГГц (5,15-5,25 ГГц, 5,25-5,35 ГГц, 5,725-5,825 ГГц).
Швидкість передачі даних	1 Мбіт/с, 2 Мбіт/с, 5.5 Мбіт/с, 11 Мбіт/с (lib), 54 Мбіт/с (Па), 54 Мбіт/с (11 g)
Безпека мережі та даних	Потоковий алгоритм шифрування на основі на RC4 для захисту даних, перевірки на цілісність і аутентифікації. Обмежені можливості по розподілу ключів.
Дальність дії	Від 50 до 500 метрів в залежності від умов

Гідність	Бездротова передача даних зі швидкістю дротових аналогів, безліч програмних напрацювань, невисока вартість адаптерів і точок доступу.
Недостатки	Недостатня захищеність при застосуванні стандартних засобів, зниження швидкості в залежності від дальності і завантаження мережі

Таблиця 2.1 Основні характеристики мереж стандарту 802.11

Роботи над стандартом 802.11, пов'язаних з технологіями бездротової передачі даних, організованих за принципом Ethernet, велися з 1997 в інституті IEEE. Найбільш популярним в даний час є стандарт 802.11 b, що входить в сімейство 802.11. Перевагою є використання частотного діапазону 2,4 - 2.5 ГГц в якому для роботи в більшості країн світу не потребує ліцензування. Стандарт 802.11 передбачає два режими роботи: кожен з усіма (ad-hoc) і з використанням точки доступу (AP) або центральній станції (infrastructure).

В режимі ad-hoc кожен клієнт мережі взаємодіє безпосередньо з іншим клієнтом (Рис. 2.1).

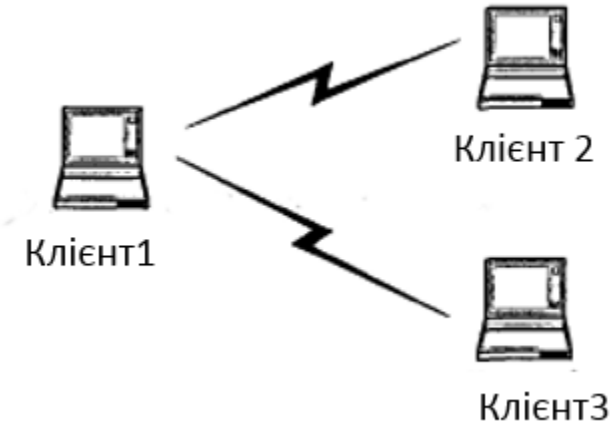


Рисунок. 2.1 Режим без використання центральної станції

В даному режимі всі клієнти повинні знаходиться на відстані, що допускає передачу інформації. Якщо клієнт захоче встановити зв'язок з клієнтом, розташованим за межами мережі ad-hoc, то один з членів мережі повинен функціонувати як шлюз і здійснювати маршрутизацію.

У режимі з використанням центральної станції весь потік інформації йде через точку доступу (AP). Точка доступу діє подібно Ethernet-мосту, забезпечуючи маршрутизацію в іншу дротову або бездротову мережу (див. Рис. 2.2).

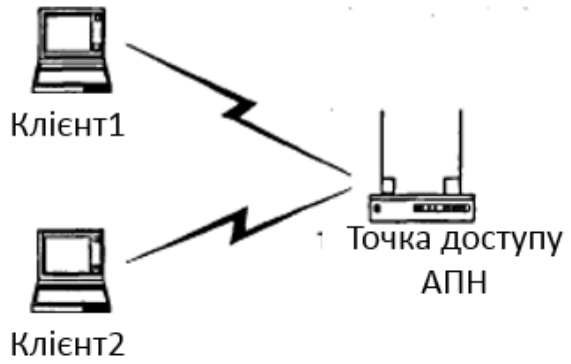


Рисунок. 2.2 Режим з використанням центральної станції

Перед тим як почати обмінюватися даними бездротова станція і точка доступу повинні встановити з'єднання. Тільки після того, як встановлено з'єднання дві бездротові станції можуть обмінюватися дані. Процес встановлення з'єднання проходить в два етапи і включає в себе три стани, в яких може знаходитися станція:

1. Нерозпізнана і несполучена;
2. Розпізнана і сполучена;
3. Розпізнана і сполучена.

Для переходу з одного стану в інший бік обмінюються - повідомленнями, званими керуючими фреймами. Точка доступу розсилає спеціальний керуючий фрейм - маяк (beacon management frame). На стороні клієнта відбувається збір таких фреймів від точок доступу, що знаходяться в зоні зв'язку. Клієнт так само може послати кадр -запит (probe request management frame) для того, щоб знайти точку доступу з певним номером SSID. Після визначення точки доступу сторони

починають процедуру взаємної аутентифікації, шляхом обміну керуючими фреймами. Після успішної аутентифікації клієнт переходить в наступну стадію - аутентифікований і несоединенный. Для переходу в третій стан клієнту необхідно надіслати запит на підключення (association request frame) на що точка доступу повинна в свою чергу надіслати підтвердження (association response frame). Після цього станція клієнта стає повноправним членом бездротової мережі і може обмінюватися даними з іншими станціями мережі.

2.2. КЛАСИФІКАЦІЯ ТИПІВ АТАК НА РАДІОКАНАЛ

До можливих ризиків при використанні мережевої інфраструктури стандарту 802.11 b відносяться атаки на конфіденційність інформації, цілісність і доступність мережевих ресурсів.

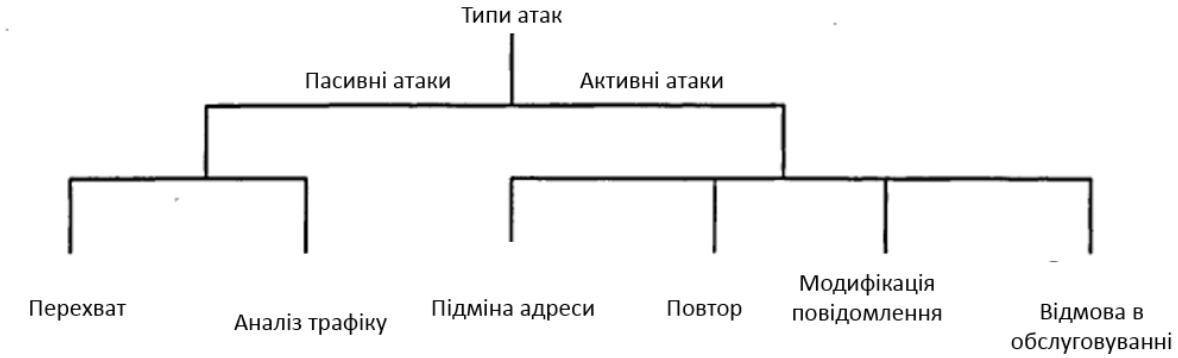


Рисунок. 2.3 Типи атак на бездротову мережу стандарту 802.11

Як показано на (Рис. 2.3), атаки, спрямовані на порушення безпеки бездротової мережі діляться на активні і пасивні. Вони, в свою чергу, поділяються на кілька підкласів.

Пасивні атаки - до цього класу належать атаки, в ході яких неавторизована сторона просто отримує доступ до даних, не модифікуючи їх. Для системного

адміністратора неможливо встановити факт пасивної атаки. Пасивними атаками вважається як перехоплення даних, так і застосування аналізатора трафіку.

Перехоплення - Атакуюча сторона переглядає зміст повідомлень, що передаються в мережі. Як приклад можна привести перехоплення повідомлень між двома робочими станціями в мережі або між станцією і точкою доступу.

Аналіз трафіку - в даному випадку застосовується підхід з фільтрацією трафіку за певними критеріями. Проводиться накопичення статистики за повідомленнями, що містить заздалегідь відомі фрагменти.

Активні атаки - атаки, при яких неавторизована сторона виробляє модифікацію повідомлень. Можна виявити факт атаки даного класу, але не завжди можливо запобігти її. Активні атаки виіляються на чотири підкласу: підміна адреси, повтор, модифікація повідомлення і відмова в обслуговуванні.

Підміна адреси - шляхом підміни адреси атакуюча сторона може отримати всі або частину привілеїв авторизованого користувача.

Повтор - атакуюча сторона перехоплює повідомлення і передає їх під виглядом авторизованого користувача

Модифікація повідомлення - проводиться модифікація повідомлення шляхом додавання, вилучення або модифікації даних.

Відмова в обслуговуванні - атакуюча сторона шляхом формування повідомлень певного виду унеможливлює нормальне використання або управління бездротовою мережею.

2.3. АНАЛІЗ СТАНДАРТНИХ ЗАСОБІВ І МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ В РАДІОКАНАЛІ 802.11

Основою захисту даних, що передаються в бездротових мережах, є протокол WEP. Як випливає з результатів досліджень протокол WEP не володіє достатньою стійкістю і має ряд структурних недоліків.

Одним з методів захисту інформації в мережі є приховування імені мережі або SSID. Однак, у багатьох рішеннях, пропонованих постачальниками бездротового обладнання, зокрема в обладнанні фірми Lucent, присутній ряд уразливості в системах, що забезпечують контроль доступу до мережі. Деякі керівні кадри містять ім'я мережі або SSID, причому ці повідомлення, що розсилаються як точками доступу, так і клієнтами, є широкомовними і не зашифровуються. Вид керуючого фрейму, що містить SSID, залежить від конкретного виробника. В результаті атакуюча сторона отримує інформацію про ім'я мережі, що в поєднанні з підібраним секретним ключем дає доступ до захищеної мережі. Цей недолік проявляється в не залежності від активації режиму шифрування з допомогою протоколу WEP, так як керуючі фрейми при цьому передаються відкритим текстом.

Механізм захисту, заснований на застосуванні таблиці MAC-адрес для станцій, яким дозволений доступ, теоретично гарантує високу стійкість при використанні надійної ідентифікації клієнта. Але на практиці так не відбувається, в результаті того, що MAC-адреса повинна передаватися у відкритому вигляді, навіть у разі активації протоколу WEP. Всі сучасні мережеві карти стандарту 802.11 мають можливість програмної зміни MAC-адреси. Таким чином, при перехопленні адреси, якій дозволений доступ, можлива підміна значення MAC на станції атакуючої сторони і отримання доступу в захищену мережу.

Злом протоколу аутентифікації із загальним секретним ключем можна здійснити за допомогою пасивної атаки з перехопленням фреймів, що передаються

в процесі взаємної аутентифікації. Можливість атаки визначається недоліками, зазначеними в і статичною структурою

протокол. Єдина відмінність між повідомленнями при аутентифікації полягає в вмісті перевірочного тексту.

Спочатку атакуюча сторона перехоплює другий і третій керуючий фрейм, що передаються в процесі аутентифікації. Другий фрейм містить перевірочний текст в незашифрованому вигляді, а третій той же текст, але вже зашифрований за допомогою загального секретного ключа. Таким чином, атакуючій стороні стає відомий незашифрований текст P, той же текст, але вже зашифрований З і значення IV, яке передається в незашифрованому вигляді. Далі можна обчислити псевдовипадкову послідовність WEPKIV, згенеровану із застосуванням секретного ключа к і значення вектора ініціалізації IV використовуючи формулу 2.1.

WEPKM=C®P (2.1)

Розмір псевдовипадковою послідовності буде точно таким же, як і розмір кадру аутентифікації. При цьому всі елементи кадру заздалегідь відомі: номер алгоритму, номер послідовності, код стану, ідентифікатор елемента, довжина і контрольний текст.

Таким чином, атакуюча сторона має можливість успішно аутентифицироваться в захищеній мережі навіть при невідомому секретному ключі К. Атакуюча сторона надсилає запит до тієї точки доступу, до якої потрібно підключитися. Точка доступу відповідає керуючим фреймом, що містить перевірочний текст. Атакуюча сторона розраховує тіло фрейму аутентифікації шляхом обчислення XOR (виключає «або») від значень отриманого випадкового тексту R і послідовності WEP. Наступним кроком необхідно обчислити нове значення контролю цілісності (ICV). Для цього застосовується методика, докладно описана в розділі «Активна атака з метою підміни трафіку». Після цього станція стає авторизованою для захищеної мережі. Якщо в захищеній мережі

застосовується протокол WEP, то атакуючій стороні не вдасться обмінюватися інформацією з іншими станціями без застосування спеціальних засобів.

Основні проблеми, пов'язані з безпекою бездротових мереж стандарту 802.1 lb

1. Засоби безпеки, вбудовані виробником обладнання, дуже часто не використовуються. Незважаючи на недоліки механізмів безпеки, реалізованих різними виробниками у своїх продуктах, їх використання знижує ймовірність виникнення проблем з безпекою даних.

2. Діапазон значень IV малий або використовується статичний IV. В виду того, що IV - 24 бітне число, можлива атака, заснована на дешифрування повідомлень, зашифрованих за допомогою одних і тих же значень ключового потоку (key stream).

3. Довжина криптографічного ключа мала довжина ключа в 40 біт не адекватна для захищених систем. В даний час рекомендована довжина не менше 80 біт. Велика довжина ключа ускладнює атаку методом перебору.

4. Використання загального криптографічного ключа використання загального ключа може призвести до проблем в області захисту інформації. Безпека мережі залежить від збереження секретного ключа, який має бути відомий кожній станції.

5. Криптографічний ключ не може бути змінений автоматично і з потрібною частотою Криптографічний ключ необхідно часто змінювати для попередження можливих атак методом перебору.

6. Слабкість алгоритму RC4 внаслідок особливостей його застосування в алгоритмі WEP Так як значення IV є частиною ключового потоку для алгоритму RC4 і передається у відкритому вигляді, може бути зроблена атака з метою отримання криптографічного ключа. Даний недолік алгоритму RC4 не проявляється у випадках, відмінних від WEP, так як не відкривається частина ключового потоку і не проводиться перезапуск алгоритму для кожного пакету даних.

7. Алгоритм захисту цілісності має недоліки Алгоритми лінійної блочною структурою, подібні CRC32 не можуть забезпечити надійний захист цілісності для

застосування в криптографії. Можлива зміна вмісту пакета. Лінійні алгоритми схильні до атаки, спрямованої на підміну вмісту пакету. Використання в процесі підготовки пакету некриптографічних алгоритмів часто полегшує можливі атаки на зашифровану інформацію.

8. Недоліки в системі аутентифікації на основі списку MAC адрес При використанні аутентифікації на основі списку MAC - адрес вкрадене пристрій може безперешкодно увійти в мережу, так як не здійснюється перевірка користувача.

9. Проблеми при використанні аутентифікації на основі ідентифікатора SSID при аутентифікації на основі ідентифікатора мережі можливе перехоплення пакетів з подальшим отриманням значення SSID.

10. Недоліки аутентифікації влаштування на основі загального криптографічного ключа Одностороння аутентифікація на основі запиту-відповіді із застосуванням загального криптографічного ключа вразлива до атаки, так як може бути здійснено перехоплення і аналіз переданих даних. Потрібна додаткова аутентифікація користувача для визначення його прав на доступ в мережу.

2.4. ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ ПРОТОКОЛУ WEP

У зв'язку з зростанням і розвитком індустрії бездротового доступу постало питання про надійність передачі і ступеня захищеності радіомережі [17]. При пересиланні даних по радіохвилях вони можуть бути легко перехоплені і змінені. Таким чином, необхідний механізм безпеки для забезпечення захисту інформації в радіоканалах.

Зазвичай в мережах стандарту 802.11 відбувається взаємодія між клієнтською станцією і точкою доступу (AP - Access Point), використовуючи радіохвилі. Якщо перешкод (стін, штучні або природні перешкоди) між AP і клієнтської станцією не екранують радіосигнал, то пряма видимість не потрібно. Поряд зі специфікаціями з

передачі даних стандарт визначає протокол WEP (Wired Equivalent Privacy), що слугує механізмом захисту даних при передачі по радіоканалу від перехоплення. Захист інформації здійснюється за допомогою зовнішнього сервісу управління ключами, створеними для процесів шифрування і розшифровки повідомлень, що передаються по мережі. Серед основних властивостей алгоритму WEP можна відзначити:

- Стійкість до підбору ключів. Безпека інформації забезпечується алгоритмом, базується на складності знаходження секретного ключа при атаці методом перебору можливих комбінацій (brute-force attack). Стійкість залежить від довжини секретного ключа і частоти зміни ключів.
- Самосинхронізація. Алгоритм WEP дозволяє здійснювати синхронізацію для кожного послання. Ця властивість особливо важлива для алгоритмів шифрування використовуваних на канальному рівні, у випадках, коли накладаються підвищені вимоги до надійності передачі і висока ймовірність втрати інформаційних пакетів.
- Ефективність для реалізації. Алгоритм WEP може бути реалізований як на апаратному, так і на програмному рівні.
- WEP є не обов'язковим компонентом стандарту IEEE 802.11 і, при відсутності в ньому необхідності, може не реалізовуватися в пристроях бездротового зв'язку.

Стандартна система аутентифікації має недоліки, основні з них наведені нижче:

1. Необхідність доставки загального секретного ключа WEP, неможливість частої зміни ключа;
2. Підміна MAC адреси;
3. Перехоплення пакетів з подальшим отриманням значення SSID;
4. Одностороння аутентифікація на основі запиту-відповіді із застосуванням загального криптографічного ключа.

Система аутентифікації радіоканалу стандарту 802.11 b побудована на основі стандарту IEEE 802.їх. 802.їх визначає, як використовувати розширений протокол аутентифікації (Extensible Authentication Protocol - EAP).

Серед EAP методів розроблених спеціально для бездротових мереж варто особливо виділити сімейство, засноване на стійких паролях.

Алгоритм SPEKE був розроблений з метою подолати проблеми, пов'язані з низьким ступенем безпеки і високою складністю в реалізації властиві методів аутентифікації, заснованим на сертифікатах. Дослідження призвели до розробки нового сімейства алгоритмів аутентифікації на основі паролів, причому були усунені недоліки, присутні в традиційних алгоритмах, що використовують паролі. Тоді ж був введений термін "стійкий пароль", що показує приналежність алгоритму до даного сімейства. Головне достоїнство алгоритмів на основі стійких паролів в тому, що обидві сторони можуть довести один одному, що вони знають секретний пароль, при цьому не викриваючи його при третьої сторони, яка може перехоплювати повідомлення. Алгоритми на основі стійких паролів дозволяють зробити захищену аутентифікацію із застосуванням коротких, легко запам'ятовуються паролів. Основою таких алгоритмів є метод обміну Діффі-Хелмана (Diffie-Hellman). Метод Діффі-Хелмана дозволяє двом сторонам створювати ключ шифрування, причому третя сторона, яка може мати можливість перехоплювати повідомлення, не зможе отримати цей ключ.

Безпека методів, застосованих у криптографічних алгоритмах системи аутентифікації, базується на припущенні, що зведення в ступінь є односторонньою функцією, основною небезпекою є можливість для атакуючої сторони обчислити дискретний логарифм від результату. Всі відомі методи обчислення дискретного логарифма вимагають великих обсягів предвычислений для кожного конкретного значення модуля.

Алгоритми SPEKE і DH-EKE володіють нижче перерахованими характеристиками.

1. Запобігають можливість відкладеної (off-line) атаки по словнику пароль

2. Протистоять атаці за словником в реальному часі
3. Забезпечують можливість взаємної аутентифікації
4. Мають вбудовану систему обміну ключів
5. Немає необхідності в довготривалих (persistent recorded secret data) секретних або специфічних (sensitive host-specific data) даних.

Можливість здійснення атаки по словнику в реальному часі (On-line dictionary attacks) може бути легко виявлено і попереджено, наприклад простим підрахунком кількості невдалих входів в систему. Але проблема відкладеної атаки за словником на пароль становить велику небезпеку. Атакуюча сторона може маскуватися під другого учасника аутентифікації, або перехоплювати повідомлення, якими обидві сторони обмінюються при взаємної аутентифікації. Витік будь-якої, навіть незначної частини інформації при обміні може призвести до успішної атаки. Алгоритм повинен бути стійкий до атак такого типу, навіть при застосуванні паролів невеликої довжини.

Взаємна аутентифікація бажана для того, щоб кожна з двох сторін була впевнена, що інша знає пароль.

У той же час, використовуючи пароль генерується ключ сесії для забезпечення безпеки обміну даними між двома сторонами. Необхідність у вбудованій системі обміну ключів при аутентифікації детально обговорюється в [33]. Основна ідея полягає в тому, що, розділяючи кроки аутентифікації і обміну ключами, створює можливість третій стороні здійснити атаку, перехоплюючи повідомлення. Захищений обмін ключами вимагає спільної участі обох сторін, і повинен бути невід'ємною частиною процесу.

Відсутність потреби у зберіганні довготривалих секретних даних означає, що користувачеві не потрібні додаткові симетричні, відкриті або приватні ключі. Існує безліч способів для створення захищеного каналу, через який може бути переданий у відкритому або хешированном вигляді пароль. Методи, засновані на пароль (password-only method) дозволяють використовувати пароль як незалежний фактор

і спростити налаштовувану частина системи. З одного боку довготривалі дані необхідно згенерувати, поширити і захистити при зберіганні, що створює додаткові проблеми. З іншого боку секретні дані не повинні бути розкриті, зашифровані дані треба оберігати від несанкціонованого втручання. Отже, потрібне застосування спеціальних захищених областей пам'яті, що погіршує систему безпеки і створює додаткові можливості для порушення захисту. Системи, в яких безпека пароля залежить від збереженого ключа набагато простіше при розробці, але вони лише переміщують основу безпеки з пароля на ключ. Якщо ключ викрадений, пароль може бути скомпрометований. Відмова від власних ключів позбавляє від цієї проблеми, також зникає необхідність використовувати захищене сховище.

Алгоритми SPEKE і DH-EKE володіють всіма вищепереліченими достоїнствами і мають інші бажані характеристики, які будуть розглянуті нижче.

2.5 ОПИС АЛГОРИТМІВ SPEKE І DH-EKE

Алгоритми SPEKE і DH-EKE базуються на методі обміну ключів Діффі-Хелмана. Класичний обмін за алгоритмом DH дозволяє двом сторонам без попередньої домовленості створити загальний секретний ключ сесії.

Сам по собі DH не передбачає аутентифікації і схильний атаці 'типу" людина в середині".

Алгоритми SPEKE і DH-EKE входять в один з видів протоколів аутентифікованого обміну ключами. Використання DH захищає пароль від відкладеної атаки за словником, тоді як механізм використання пароля в цих алгоритмах запобігає можливість атаки "людина в середині", як описано в роботі [21] описано яким чином обмін збільшує ступінь захисту загального секретного пароля за рахунок значно більшого ключа сесії. Дві сторони, які спільно використовують пароль невеликої довжини (S), можуть провести аутентифікацію використовуючи незахищений канал, довести один одному знання S і згенерувати новий великий ключ сесії (До).

Ці алгоритми використовують арифметику всередині великої кінцевої групи. Кілька видів таких груп можуть бути використані в DH, однак ми обмежимося розглядом Zm , де т є великим простим числом.

ВИСНОВКИ ДО РОЗДІЛУ 2

1. Розроблено методи поліпшення системи безпеки заснованої на алгоритмі WEP;

2. Створено класифікацію типів атак, наведені методи вирішення проблем з безпекою даних для кожного з видів атак;

3. Розроблено методи, що дозволяють усунути знизити ймовірність успішних атак на стандартну систему безпеки;

4. Розроблено засоби захисту від атак на системи аутентифікації заснованих на алгоритмах SPEKE і DH-EKE;

5. Створено класифікацію типів атак на систему аутентифікації і розроблені методи захисту;

РОЗДІЛ 3. РОЗРОБКА МОДЕЛІ

3.1 АРХІТЕКТУРА ЗАБЕЗПЕЧЕННЯ

Поряд з багатьма перевагами в алгоритмі WEP є недоліки в області безпеки [6, 7, 10]. У WEP використовується поширений симетричний алгоритм генерації псевдовипадкових чисел RC4 PRNG (Ron's Code 4 Pseudo Random Number Generator) [5]. Однак реалізація містить ряд недоробок в області безпеки. Дані недоліки дозволяють здійснювати ряд як активних, так і пасивних атак по перехопленню і підміні повідомлень, що передаються по бездротових мережах.

У протоколі реалізований класичний 40 бітний ключ і 24 бітний IV, проте конкретними виробниками зазвичай розробляються розширені версії, що підтримують велику довжину ключа. Чим коротше довжина ключа, тим більше він є схильним атаці шляхом перебору комбінацій (brute-force attack), що цілком під силу більшості сучасних комп'ютерів. При збільшенні розрядності секретного ключа, приміром, до 128 біт, перебір стає неможливим навіть для спеціальних обчислювальних систем. Однак залишаються можливості для атак, що не використовують метод перебору і зводять нанівець всі переваги довгого ключа.

В результаті за відносно невеликий проміжок часу можливе перехоплення двох пакетів даних, які зашифровані однією і тією ж ключовою послідовністю. Далі можливий статистичний аналіз для відновлення вихідного незашифрованого тесту, що міститься в одному повідомленні. У випадку вдалого підбору, провівши операцію «виключне АБО» (XOR) над зашифрованим повідомленням і розпізнаним текстом зловмисник відновлює відповідну ключову послідовність, що дозволяє йому переглядати всі інші зашифровані повідомлення, зашифровані з допомогою даного IV:

$$M \oplus C = M \oplus (M \oplus RC4(IV, K)) = RC4QV, K)$$

Навіть якщо не вдасться розпізнати звістку контекст повідомлення, про нього можна здогадатися, використовуючи передбачувану структуру і надмірність IP

трафіку. В подальшому знання структури вмісту зашифрованого текст дозволяє звузити область пошуку можливого контексту. Так як зловмисник має два або декілька зашифрованих пакетів одним і тим же IV, він має можливість застосувати операцію XOR до вмісту і виявити відмінності і збіги в структурі:

Рисунок 3.1. Схема аутентифікації стандарту

Іншими словами застосування операції XOR над двома такими зашифрованими повідомленнями дозволяє виключити вплив ключової послідовності і аналізувати різницю незашифрованих даних (М/ Ф М2), що дає набагато більше шансів у розкритті вмісту пакетів методом статистичного аналізу.

Якщо зловмисник зміг зіставити вихідний і зашифрований текст, то він, очевидно, зможе згенерувати ключову послідовність. Володіючи цими відомостями не складно організувати передачу зашифрованого трафіку на станцію жертви, причому приймач повідомлень пізнає приходять пакети як коректні.

Дана атака може проводитися і іншим способом. Навіть якщо зловмисник не досяг повної розшифровки вмісту пакета, він може довільно змінювати значення

бітів у повідомленні, потім додавати обчислене значення контролю цілісності ICV для отримання коректної версії модифікованого пакета. Операція XOR має властивість дистрибутивності: c(x ⊕ y) = C(x) ⊕ c(y) для будь-яких x і y. Розглянемо ситуацію, в якій проведено перехоплення пакету з даними, де зашифровані дан.:

При цьому можливе створення такого зашифрованого повідомлення з яке відповідає р.. де, причому а може бути підібрана атакуючою стороною. Далі з'являється можливість підміни пакету з даними:

(A)->B: (IV || C)

в цьому випадку станція в отримає змінений пакет даних р ' з коректним значенням контролю цілісності.

Можлива ситуація, в якій зловмисник, перехоплюючи трафік в мережі, має уявлення тільки про заголовку кадру, а не про вміст повідомлення. Наприклад, або заздалегідь відомий або обчислений IP адреса жертви. Маючи цю інформацію, зловмисник може замінити відповідні біти пакету' для підміни IP адреси на адресу станції знаходиться під його контролем, за умови, що мережа, на яку ведеться атака, підключена до мережі Інтернет. Далі пакет потрапляє на точку доступу, що з'єднує бездротову мережу з Інтернет, розшифровується, і у відкритому вигляді пересилається на комп'ютер зломщика. При цьому модифікований пакет переміщається з бездротової мережі в Інтернет, отже, він не буде затриманий більшістю стандартних мережевих екранів.

Для здійснення даної атаки недостатньо просто замінити IP адресу одержувача пакету, необхідно щоб контрольна сума зміненого пакету була коректною. Припустимо, що DL і DH - це дві 16-бітні частини вихідного IP адреси одержувача, їх необхідно замінити на ' L і D H. Позначимо значення старої контрольної суми як S, причому її значення не обов'язково може бути відомо. Тоді нове значення обчислюється за формулою:

S' = S + DL + DH-D L-D H

Якщо значення S заздалегідь відомо, то нескладно обчислити значення S 'і модифікувати пакет операцією XOR зі значенням S ⊕ S'. Якщо S заздалегідь не відомо, то завдання набагато складніше. Відомо значення E = S'-S, необхідно обчислити Δ = S ⊕ S'. При використанні методів статистичний аналіз і володіючи певною структурою повідомлення, велика ймовірність підбору потрібного значення.

Відносно мала кількість можливих значень IV дозволяють атакуючій стороні побудувати таблицю розшифровки. При вдалій спробі розшифровки вмісту будь-якого пакету даних стає можливим відновити-ключову послідовність, - згенеровану при поточному IV. Ця ключова послідовність потім може бути використана для розшифровки всіх інших пакетів, які використовують те ж саме значення IV. При досить добре відпрацьованої технології статистичного аналізу зловмисник може побудувати таблицю відповідності IV векторів і відповідних їм ключових послідовність. Така таблиця буде містити близько 2 (більше 16 мільйонів) записів, що складе обсяг близько 24 Гб. Користуючись цією таблицею, зловмисник зможе розшифрувати будь-який пакет без зусиль, досить з'ясувати тільки значення ключової послідовності по його IV.

3.2. МЕТОДИ ВИРІШЕННЯ ПРОБЛЕМ З БЕЗПЕКОЮ

За повідомленнями аналітиків на сьогоднішній день лише в 40% бездротових мереж стандарту 802.11 активований протокол WEP [8, 12, 13]. Це призводить до втрати конфіденційності переданої інформації і робить можливим здійснення атак на мережеву інфраструктуру. Для протидії необхідно використання протоколу WEP і якомога частіше міняти секретний ключ. При конфігуруванні необхідно встановлювати довгі, - стійкі до підбору ідентифікатори SSID.

Застосування фільтрації MAC адрес або використання WLAN дозволить заборонити доступ неавторизованим бездротових карт. Необхідно обов'язково закрити доступ до інтерфейсу конфігурування точок доступу в бездротовій мережі. Використання програми антивіруса і мережевого екрану усуне можливість появи на клієнтських машинах сторонніх програм-шпигунів і перехоплювачів.

Об'єднуючи захист за допомогою брандмауера і технології IPsec, SSH або SSL можливо з високою часткою ймовірності виключити можливість перехоплення інформації і запобігти доступ для невпізнаних клієнтів.

Основні зусилля додаються в області розмежування функцій шифрування і аутентифікації для того, щоб не було необхідності у спільному використанні секретного ключа на всіх станціях бездротової мережі. Був прийнятий чорновий варіант стандарту попередньо названий Enhanced Security Network (ESN), в якій передбачений посилений варіант захищеної аутентифікації і система управління 128-бітними ключами. У системі шифрування ESN буде замінено алгоритм генерації псевдовипадкових чисел RC4 PRNG на сучасний стандарт Advanced Encryption Standard (AES). З прийняттям нової версії WEP2 рівень безпеки бездротових мереж може досягти рівня безпеки їх дротових аналогів.

3.3. РОЗРОБКА ЗАСОБІВ ЗАХИСТУ ВІД АТАК НА СИСТЕМУ АУТЕНТИФІКАЦІЇ, ЗАСНОВАНОЇ НА АЛГОРИТМІ SPEKE

В роботі обговорюються проблеми обчислення дискретного логарифма, і обговорюється вибір параметрів для основної DH аутентифікації, особливо із застосуванням коротких значень експоненти. Таблиця 3.1 - скорочена зведена таблиця, присвячена методам захисту для обох алгоритмів.

Метод захисту	Відвернена атака	SPEKE	DH-EKE
Модуль m повинен бути великим числом	Обчислення дискретного логарифма	V	V
Перевірка на Qx ! = 0, у разі не зашифрованих значень	Форсування значення К = 0	V	V
Значення m -1 повинно мати великий просто множник q.	Обчислення логарифма за методом Полінгу-Хелмана	V	V
Шифрування Qx, розбитого на частини і зібраного у випадковому порядку	Витік інформації з значення Es(Qx)		V
База g повинна бути першоподібним коренем від т.	Розподілена атака на Es (Qx)		V
База повинна бути генератором для q	Розподілена атака Qx	V	
База у вигляді Sx mod p	Атака типу «пароль в експоненті»		
Необхідно шифрувати Qx при перевірці К	Підбір пароля використовуючи Qx, Rx словник паролей		V

Використання одностороннього хешування значення K	Атака на обмеження значень	V	V
Перший біт m повинен дорівнювати 1	Розподілена атака на Ек(Qx)		V
Шифрування значень Qa,Qb	Обмеження по підгрупам для K		V
Переривання роботи, якщо K малого порядку	Обмеження по підгрупам для K	V	

Таблиця 3.1 Методи захисту для обох алгоритмів

Можливі атаки на процес DH-обміну можна умовно розділити на наступні класи:

- Обчислення дискретного логарифма
- Витік інформації
- Обмеження по невеликих підгрупах

В атаці "обчислення дискретного логарифма" проводиться зворотне - перетворення від зведення в ступінь по модулю m, з метою відновити показник ступеня i, в кінцевому рахунку, пароль S. трудність цих обчислень залежить від розміру і властивостей числа m. стійкість алгоритму до даної атаки грунтується на практичній неможливості подібного обчислення.

Необхідно відзначити, що перехоплення значень експоненти, можливо зашифрованою, не призводить до витоку інформації про пароль S. Витік навіть одного біта інформації про пароль може бути критичною, у разі якщо застосовується атака з підбором по словнику, дозволяє розділити можливі паролі на дві групи: відповідні і свідомо неправильні. Такий тип атак - «розподілена атака» (partition attack) може зменшити словник великого розміру до кількох значень за відносно мала кількість проходів.

Нарешті, атакуюча сторона, яка знає структуру Zm, може бути здатна обмежити область можливих значень K до розміру невеликий підгрупи, яка дозволяє здогадатися про значення або застосувати атаки перебором. При аналізах безпеки алгоритму Діффі-Хелмана (Diffie-Hellman) передбачається, що K завжди розташоване з рівномірною ймовірністю в Zm. Це припущення є невірним, так як, починаючи з першого зведення g в ступінь, що є випадковим числом, відбувається потрапляння результатів в меншу підгрупу, принаймні, в половині випадків. На цій закономірності грунтується атака "обмеження по невеликих підгрупах".

Атака через обчислення дискретного логарифма

Безпека методів, застосованих в алгоритмах, базується на припущенні, що зведення в ступінь є односторонньою функцією, основною небезпекою є можливість атакуючої сторони обчислити дискретний логарифм від результату. Всі відомі методи обчислення дискретного логарифма вимагають великих обсягів предвычислений для кожного конкретного значення модуля.

Розмірність модуля - основа захисту. На сьогоднішній день не відомі методи обчислення дискретного логарифма розмірністю більшої близько сотні біт, проте цілком ймовірно, що в недалекому майбутньому можливі успішні атаки на модулі розміром в 512 біт. Десь у діапазоні від 512 до 1024 біт знаходиться ідеальний розмір модуля, збалансований за вимогами безпеки і швидкості обчислень, для конкретних додатків.

Більше того, потрібно правильно підібрати модуль т з метою запобігти можливість швидкого обчислення дискретного логарифма. Якщо m-1 має великий простий множник q, то він може протистояти атаці на обчислення дискретного логарифма Полига-Хелмана (Pohlig-Hellman). Використання безпечних простих чисел у вигляді m = 2q+l, є одним із способів подолати цю вразливість.

Передбачається, що необхідні предвычисления дискретного логарифма виконані для певного модуля, в атаці на основі' підбору пароля необхідно

розрахувати конкретний логарифм для кожного запису в словнику паролів, поки не буде знайдено правильне значення. Будь-яка сесія, що використовує модулі є вразливою для атаки з логарифмування. Таким чином, необхідно дотримуватися ситуацію робить проблему обчислення дискретного логарифмування як можна більш важкою. В цьому разі здійсненність преобчислювань є першорядною проблемою.

Розподілена атака

У методі Діффі-Хелмана використовується група Zm , де m - велике ціле число, причому m-1 має великий простий множник q. При цьому g є первісним коренем від m. На практиці g має бути простим для того, щоб запобігти атаці. Третя сторона може здійснити пробне дешифрування Es(gRx mod m) використовуючи словник паролів Si Es -симетрична функція шифрування, що використовує ключ Si. Якщо g не просте число, не вірне Si підтвердитися простим результатом. В загальному випадку для запобігання атаки на DH-EKE зашифроване значення Qx не повинно містити передбачуваної структури. Умова, що g є простим числом, дозволяє домогтися рівномірного розподілу значень всередині Zm.

- g має бути простим числом

Також необхідно звернути увагу на можливі недоліки методу шифрування як такого, зокрема необхідно заповнювати порожні повідомлення випадковим текстом, що відноситься до обмежень, що накладається на функцію Es. З урахуванням всього цього інші рекомендовані обмеження для DH-EKE:

- m повинна бути виду m-1
- розбиття на блоки при шифруванні Es у випадковому порядку

Для алгоритму SPEKE не потрібно цих обмежень, так як в ньому не використовується симетричне шифрування.

У алгоритмі SPEKE не потрібне використання простої основи. Якщо основа f(S) - випадковий член групи Zm, сторона, що перехоплює значення може їх

перевірити на належність до малих підгрупах. Якщо результат є першоподібним коренем від т, значить база так само просте число. Для безпечних цілих m це означає розкриття 1 біта інформації про пароль S. Якщо значення т буде змінюватися,-як рекомендовано для підвищення безпеки, атакуюча сторона може отримати нову інформацію, що дозволить зменшити розмір словника для пошуку Sj.

У разі якщо для будь-якого значення S, підстава f(S) є генератором великої підгрупи, то для атакуючої сторони неможливо отримати потрібну інформацію з результату. У подальших міркуваннях ми будемо припускати використання в якості базису великого простого числа.

Так як в алгоритмі SPEKE не шифруються значення Qx, формальний аналіз набагато спрощується в порівнянні з DH-EKE.

Атака на основі обмеження результату по підгрупах

В атаці на основі обмеження по підгрупах результат досягається у звуженні області можливих значень До до розмірів невеликого масиву, це досягається, якщо змусити одну або обидві сторони використовувати обмежений набір значень t невеликої розмірності, як підстави для зведення в ступінь. Використання безпечної простого значення т = 2q+l зменшує, але повністю не скасовує ймовірність присутності невеликих підгруп, як показано на Рис. 3.3. Навіть при застосуванні безпечного простого цілого m, Zm все ще містить невелику підгрупу G2. Розглянемо два можливих види атак.

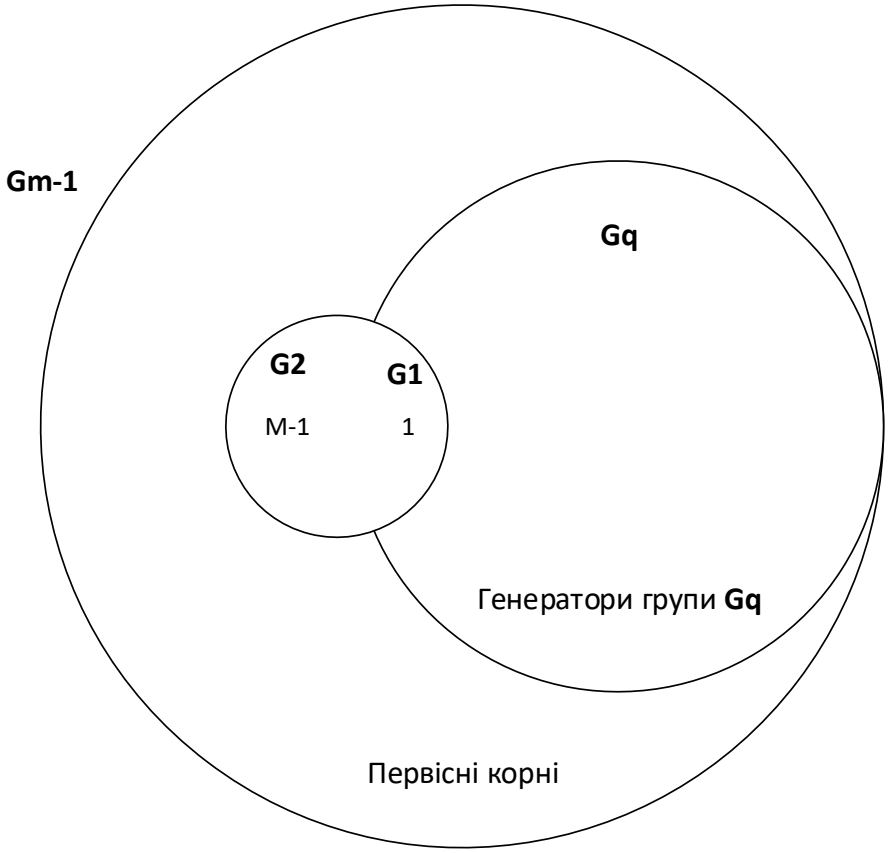


Рисунок. 3.2 Підгрупи Zm для m=2q+1

В атаці з перехопленням повідомлення обидві сторони не здогадуються, що хтось перехоплює і модифікує повідомлення. Знаючи, що є невеликим первообразным коренем m - 1, третя сторона перехоплює повідомлення від обох сторін Qa і Qb і пересилає Qa(m-1)/t Qb(m-1)/t адресатам. Це дозволяє перетворити статечні значення в генератори невеликих підгруп Gt.

Обидві сторони змушені згенерувати загальне значення К, яке буде обмежено всередині невеликої підгрупи Gt. Третя сторона, в цьому випадку, має можливість підібрати К шляхом перебору. Для подолання даної атаки рекомендується використовувати підгрупу з великим простим порядком, при цьому обмеження зведеться до підгрупи Gt, яку можна однозначно детектувати. Альтернативним захистом є перевірка на приналежність до невеликих підгруп значення К, за умови відомих множників m-1. Якщо до входить в таку групу, необхідно скасувати процедуру з'єднання.

Дана атака так само може мати місце, якщо третя сторона маскується під учасника з'єднання і посилає значення QB малого порядку t іншій стороні, це актуально у випадку SPEKE або DH-EKE, якщо значення Qв не шифрується. Така одностороння атака, також дозволяє отримати K обмежене всередині Gh що дає третій стороні шанс з 1/t -вірогідність I/t вгадати значення K. При невеликому – значенні t шанси підібрати K збільшуються. Дана атака працює тільки проти алгоритму SPEKE, так як значення Qa і Qb при передачі не шифруються.

Один із шляхів захисту від подібних атак полягає в спробі виключити невеликі підгрупи з Zm. Для цього необхідно вибирати m з безпечних простих чисел, що породжує невеликі підгрупи. Для алгоритму DH-EKE необхідно завжди шифрувати передані значення, при цьому атакуюча сторона не зможе знизити порядок Qx.

Атака з відомим ключем сесії

У роботі розглянута атака, при якій викрадений ключ сесії к використовується для проведення атаки на пароль за словником. Стійкість до цієї атаки близько пов'язана з поняттям повної прямої безпеки, завдяки якій відбувається ізоляція одного типу секретних даних від атак на інші.

В алгоритмі DH-EKE, відоме значення Ra в доповненні до відомого K дозволяє здійснити атаку по словнику з метою відкрити пароль S. Для кожного пробного пароля Si, атакуюча сторона обчислює:

$$K' = (Esi^{-1}\big(Es(g^R b)\big))^R a$$

При цьому якщо K’ = K , то відповідно Si дорівнює S. Алгоритм SPEKE так само схильний цій атаці, при якій за допомогою Ra обчислюється S. У зв'язку з цим необхідно негайно знищувати тимчасові змінні шифрування, такі як Ra і Rb.

Атака на стадії перевірки

На стадії перевірки в протоколах DH-EKE і SPEKE обидві сторони доводять один одному, що їм відомо значення загального ключа K. Через те, що K є великим

криптографічним числом, друга стадія вважається захищеною до атаки методом перебору (brute-force attack), таким чином, перевірка значення К може бути виконана традиційними метод.

Виявлення атак в реальному масштабі часу

Небезпека повторюваних в реальному масштабі часу спроб підібрати пароль може бути зменшена за умови ведення історії та підрахунку невдалих спроб підключення. Необхідно обмежити кількість невірних спроб доступу до облікових записів, вимагаючи зміни пароля, при досягненні певного порогу. Поріг повинен бути заснований виходячи з довжини пароля. Так само необхідно зберігати кількість невдалих спроб підібрати пароль як при атаці на окремий обліковий запис, так і при спробі масової атаки, при якій не досягається порогу для будь-кого з користувачів.

Часто виникає бажання пробувати відокремлювати випадкові помилки від спроб проникнення, припускаючи, що більшість помилок супроводжуються успішним входом. Проте атакуюча сторона може передбачити або спробувати затримати легітимний доступ і зробити кілька пробних спроб на цей обліковий запис до успішного входу в систему користувача. Таким чином, навіть здаються очевидними помилки повинні бути ретельно досліджені обома сторонами.

Необхідно зберігати записи невдалих спроб з'єднання, як на хост-системі, так і на користувача системи. Настроювана система повинна зберігати як мінімум список останніх невдалих спроб і передавати цю інформацію по захищеному каналу на хост-систему кожний раз, коли здійснюється успішний вхід. Хост-система так само може повідомляти користувача про кількість невдалих спроб доступу з його боку. Цей метод серйозно знижує ймовірність атаки спрямованої на підбір пароля по відношенню до обох сторін.

3.4. МЕТОДИ ЗБІЛЬШЕННЯ ШВИДКОДІЇ АЛГОРИТМІВ

Використання короткого модуля

Для збільшення швидкості операції зведення в ступінь, розмірність модуля може бути зменшена. Але так як великий розмір модуля є умовою безпеки алгоритму Діффі-Хелмана, необхідно проявити обережність при виборі оптимальної розмірності. При зменшенні розмірності модуля, наприклад до 600 біт, можливість дискретного логарифмічного перетворення зростає багаторазово. Основні аргументи за і проти наведені в таблиці 3.2.

Аргументи

За	**Проти**
Зменшення розмірності модуля дозволяє прискорити роботу алгоритму.	Зменшення розмірності модуля дозволяє провести операцію дискретного логарифмування з меншими обчислювальними затратами
Можливість дискретного логарифмування може бути зменшена при застосуванні спеціальних або часто змінюваних модулів.	Так само, для сесій встановлених із застосуванням модуля, схильного до атаки логарифмуванням, повна пряма безпека не гарантована.

Таблиця 3.2

Для синхронізації розмірності модуля для обох сторін, передбачається, що одна зі сторін вибирає цей параметр для іншої. Таким чином, постає питання в безпеці даного підходу. Третя сторона зможе, варіюючи даний параметр отримати додаткову інформацію про паролі.

Використання несертифікованих змінюваних параметрів

Наступне питання, що стосується безпеки пов'язане з необхідністю використання змінюваних параметрів. Припустимо, що одна зі сторін вибирає m і g з заздалегідь сформованого списку і пересилає їх іншій стороні перед операцією обміну. Так як в даному алгоритмі не використовується відкритий ключ, дані параметри є сертифікованими. Аргументи за і проти наведені в Таблиця 3.3.

Аргументи

Проти	**За**
Третя сторона може видати себе за учасника обміну і послати модуль у вигляді непростого або небезпечного простого числа, що дозволить здійснити атаку на пароль іншого учасника обміну	Сторона, що бере участь в обміні може здійснити ряд перевірок, в тому числі на простоту модуля, для впевненості, що параметри безпечні.
Практичні тести перевірки на простоту є імовірнісними і гарантовано працюють з невеликими або випадково вибраними великими простими числами. Третя сторона може бути здатна вибрати непросте число, яке пройде тест і таким чином атака відбудеться.	

Таблиця 3.3

Найбільш простим рішенням даної проблеми є вбудовування фіксованих безпечних параметрів в систему, де модуль є досить великим, щоб запобігти атаці, пов'язану з обчисленням дискретного алгоритму. На даний момент довжини в 1000 або 2000 біт достатньо для забезпечення довгострокового захисту. У поєднанні з

використанням короткого значення в експоненті робить рішення відповідним для більшості ситуацій.

Особливо звертається увага на наступні обмеження:

- модуль m повинен бути великим простим числом, інакше можливе прискорене обчислення дискретного логарифма
- q має бути простим числом, так як при безпечному значенні m можливо прискорене обчислення дискретного логарифма

Використання короткого значення в експоненті

Менш радикальним підходом до проблеми збільшення швидкодії полягає в зменшенні значення експоненти до достатнього для забезпечення прийнятного рівня безпеки розміру. Кількість біт в експоненті (Qa, Qb) має бути, як мінімум вдвічі більше ніж кількість біт (t), необхідного для K, зазвичай це менше, ніж кількість біт в m.

Можна використовувати два безпечних підходи, коли експонента може бути зменшена до розміру в 2t біт:

1. Використовуючи велике безпечне значення модуля m з вихідним базисом 2.

2. Використовуючи великий простий модуль m з великим простим базисом порядку q, де q має розмірність як мінімум в 2t біт.

Перший підхід застосуємо як до DH-EKE, так і до SPEKE, однак DH-EKE потребує додаткового захисту від атаки пов'язаної з обмеженням значень у невеликих підгрупах. Використання базису g = 2 дозволяє значно збільшити швидкість роботи алгоритму. Застосовуючи g = 2 необхідно відзначити, що. для цих протоколів використовуються різні безпечні прості числа. Безпечне просте число p в алгоритмі DH-EKE повинно мати первісний корінь 2, тоді як безпечне просте, підходяще для SPEKE має в ідеалі дорівнювати 2 в ступені q.

Використання великих простих підгруп, де q << m дозволяє прискорити розрахунок DH параметрів. Це застосовується для SPEKE, але не може бути використано в DH-EKE, так як для цього алгоритму потрібна проста база.

3.5. РОЗРОБКА ВДОСКОНАЛЕНОЇ СИСТЕМИ БЕЗПЕКИ, ДЛЯ РАДІОКАНАЛУ СТАНДАРТУ 802.11

Розглянемо механізм роботи системи безпеки. У структурі мережевої моделі OSI протокол 802.11b займає найнижчий (фізичний) рівень та частина вищерозміщеного канального рівня - підрівень управління доступом до середовища (MAC). У додатку стандарт визначає використання протоколу 802.2 для управління логічним каналом (LLC).

Слабкі сторони системи безпеки протоколу 802.11b викликані як чисто фізичними факторами, так і особливостями реалізації. Основними недоліками є:

- Можливість перехоплення пакета з інформацією;
- Недостатньо надійна система аутентифікації;
- Недоліки, пов'язані з шифруванням.

Можливість перехоплення пакета з інформацією.

Проблема проявляється у зв'язку з тим, що дані передаються по радіоканалу. Будь-яка станція, що знаходиться в зоні прийому сигналу, може здійснити збір інформаційних пакетів. Якщо при цьому не використовувалося шифрування, то дані можна досить тривіально витягти з окремих пакетів і - використовувати, залежно від подальших намірів перехоплює сторони не вдаючись до застосування спеціальних засобів. Для такого роду завдань досить встановити простий мережевий монітор, який дозволяє переглядати вміст пакетів і виробляє їх фільтрацію за певними ознаками, наприклад IP адресою. Ситуація ще більше погіршується тим, що не представляється можливим встановити, прослуховується в даний момент радіоканал чи ні. Таким чином, перехоплення може відбуватися абсолютно непомітно для системних адміністраторів мережі.

Недостатньо надійна система аутентифікації.

Протокол WEP визначає використання секретного ключа, який повинен бути заздалегідь відомий всім станціям мережі, інакше кажучи, наявність ключа біля станції означає, що вона пройшла процес аутентифікації. Проте, сам протокол WEP не регламентує як спосіб передачі секретний ключа, так і з якою частотою даний ключ необхідно міняти. Це призвело до того, що багато виробників обладнання не реалізують механізми по доставці ключа, змушуючи тим самим користувачів самостійно конфігурувати пристрої і вручну переносити значення ключа на всі стації мережі. Це призводить до того, що секретний ключ змінюється рідко або можливо взагалі не змінюється досить тривалий час.

Ідентифікатор SSID (Service Set Identifier) дозволяє ділити бездротову мережу класу Basic Service Set (BSS) на логічні сегменти, будучи свого роду ідентифікатором підмережі [19]. З допомогою SSID відбувається обмеження доступу для будь-якого клієнтського пристрою, який не володіє необхідним SSID. Однак найчастіше AP (точка доступу) виробляє широкомовну розсилку ідентифікатора SSID своєї підмережі. Навіть у разі відключення функції розсилки SSID, зловмисник може отримати значення SSID, аналізуючи трафік між станціями мережі.

Крім того, можна заборонити доступ на основі фільтрації MAC-адрес. Але не дивлячись на те, що всі стандартні мережні карти повинні мати унікальний MAC адресу існує програмне забезпечення або часто є апаратна можливість по заміні MAC адреси в мережевому інтерфейсі.

Недоліки, пов'язані з шифруванням.

WEP є протоколом шифрування інформації, його специфікації описані в стандарті IEEE 802.11. Цей стандарт і протокол WEP розташовані на нижчих рівнях

(фізичному і канальному) моделі OSI, це означає, що вони незалежні і прозорі для протоколів високого рівня, таких як TCP/IP.

У реалізації тієї, яка передбачена стандартом 802.11, протокол WEP має кілька слабких місць в архітектурі, які дозволяють розшифрувати дані зловмиснику [3]. У WEP використовується алгоритм шифрування RC4 в поєднанні з 64 або 128 бітним ключем, що складається з секретного ключа і значення вектора ініціалізації IV. Причина, по якій можливий злом WEP в загальному випадку не в недоліках RC4 як такого і навіть не в довжині ключа, а скоріше в невдалій реалізації самого алгоритму.

Система безпеки стандарту IEEE 802.11 потребує серйозного поліпшення. Для цього необхідно застосувати комплексний підхід до даної проблеми.

У найпростіших випадках достатньо застосування NAT маршрутизатора для з'єднань з публічними мережами, але для побудови дійсно захищеної мережі цього недостатньо. В даному списку наведені основні сфери є основою стратегії безпеки бездротових мереж:

- фільтрація вхідного і вихідного трафіку за допомогою міжмережевого екрану;
- шифрування з'єднань для віддаленого доступу;
- подвійна аутентифікація для віддаленого доступу;
- багаторівневі зони безпеки для публічно доступних ресурсів;
- засоби виявлення спроб несанкціонованого доступу.

Розглянемо систему безпеки протоколу 802.11 з точки зору даної стратегії. Важливим фактором є те, що всі поліпшення, внесені в систему безпеки, не порушують внутрішню структуру, описану в стандарті, вони лише доповнюють і покращують її. Це дозволяє добитися повної сумісності з існуючими на ринку компонентами і технологіями від різних виробників. Модульний підхід заснований на застосуванні стандартних, добре зарекомендували себе алгоритмах і залишають можливість використовувати нові технології без необхідності зміни існуючої

структури. Дана система безпеки бездротової мережі дуже добре вписується в рамки вже існуючої політики безпеки мережі.

Тепер більшість даних, що містяться в пакеті WEP, є вже зашифрованими з допомогою IPSec, що не дозволяє використовувати атаку, засновану на зіставленні заздалегідь відомого повідомлення його зашифрованому аналогу. Слід, однак, звернути увагу, що при даному підході заголовок LLC і заголовок IPSec зашифровані тільки засобами WAP, що може трохи знизити криптографічну стійкість моделі безпеки.

Так само залишаються доступними до можливого перехоплення MAC адреса, SSID, IV, Key ID і FCS. Дану інформацію неможливо зашифрувати, так як вона використовується на фізичному і канальному (підрівень MAC) рівні.

У зв'язку з тим, що основні дані захищені за допомогою алгоритмів IPSec (DEC3) і WEP (RC4), інформація, яку можна отримати, використовуючи відкриті значення SSID, IV and Key ID не принесе відчутної користі стороні здійснює перехоплення. Значенням FCS є контрольне значення CRC від MAC пакета, що використовується для контролю цілісності даних, після того як вони були передані.

Найбільшу небезпеку з точки зору безпеки являє незашифрованная передача значення MAC адреси джерела, який може бути підмінений атакуючою стороною. Тому аутентифікацію по MAC адресу слід сприймати лише як додатковий спосіб захисту від вторгнення.

У запропонованій моделі безпеки аутентифікації піддаються як користувач, так і сам пристрій. Пристрій автентифікується за допомогою значення ключа WEP. При цьому ключ повинен змінюватися досить часто і поширюватися через захищений канал. Перед тим, як пристрою будуть видані права на обмін даними через міжмережевий екран, користувач повинен пройти процедуру реєстрації в центральній базі даних управління користувачами мережі, в якій зберігаються облікові записи та політики безпеки.

Міжмережевий екран не тільки запобігає несанкціонований доступ в мережу, але і блокує широкомовні розсилки, які можуть містити дані про внутрішню структуру мережі. Зашифрований пакет IPSec в тунельному режимі не містить додаткової інформації про структуру, доступною зовнішнього перехоплення, так як вона шифрує, а потім замінює заголовок IP пакету, який містить IP адреса пункту призначення, на власний заголовок в якому вказаний IP адреса кінцевої точки - міжмережевого екрану.

В першу чергу для успішного застосування розробленої системи, при необхідності в посиленні безпеки вже наявної бездротової мережі стандарту 802.11 b або планується розгортання нової мережі, необхідно впевнитись, що протокол WEP налаштований належним чином і функціонує. Довжину ключа рекомендується встановити в 104 біт.

Наступним кроком необхідно вибрати спосіб розподілу секретного ключа. Одним з можливих рішень є застосування захищених за допомогою SSL каналів за заздалегідь заданим розкладом. У разі непридатності даного підходу в кожному конкретному випадку може бути обраний альтернативний підхід. Найкращий метод з точки зору безпеки - призначити системного адміністратора, відповідального за зміну секретних ключів на всіх пристроях, але це може призвести до того, що ключі будуть змінюватися недостатньо часто. Деякі виробники включають власні методи розподілу ключа в свою продукцію, але так як стандарт IEEE 802.11 не визначає, як саме це повинно бути зроблено, всі подібні рішення є не стандартизованими.

Далі необхідно вирішити, який міжмережевий екран найкращим чином підходить для вирішення завдань щодо забезпечення безпеки мережі.

Екран є критичним компонентом, розміщуваним між бездротовою підмережею і внутрішньою мережею.

При виборі слід звернути увагу на основні фактори:

- Міжмережевий екран повинен забезпечувати тунельний режим роботи з зашифрованим трафіком для всіх типів бездротових пристроїв, які будуть використовуватися;
- Метод аутентифікації повинен бути сумісний з центральною базою управління користувачами;
- Підтримка аутентифікації віддалених користувачів заснована на політиках безпеки, що зберігаються в базі управління користувачами.

Наступним кроком необхідно визначити чи є застосовною технологія IPSec для наявної інфраструктури. В якості альтернативи може бути застосована технологія SSL. Але в даному підході є недоліки. Так неможлива робота в тунельному режимі між-міжмережевим екраном і віддаленим користувачем, це означає, що можливе перехоплення реальних IP адрес. Протокол SSL займає більш високий рівень в стеку TCP/IP, ніж IPSec, відповідно більша кількість незашифроване інформації може бути отримано при перехопленні і аналізі пакетів. Технологія SSL первинно була розроблена як протокол для роботи в Інтернет, таким чином, деякі з додатків можуть виявитися непрацездатними в бездротової мережі.

Проведене дослідження радіоканалу стандарту IEEE 802.11 b показало, що, незважаючи на недоліки в області захисту даних, використання стандартних методів сильно знижує можливість атаки на бездротову мережу. Для забезпечення безпеки даних необхідно створення захищеного каналу зв'язку, який включає в себе наступні компоненти:

3.6 ПРАКТИЧНЕ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ

При практичних вимірах буде застосований підхід, що об'єднує експериментальні дані і теорію поширення радіосигналу в приміщенні.

Умови тестування

Тестування проводилося в офісному приміщенні, розмірами приблизно 30 на 20 м. Структура міжкімнатних перегородок - бетон з включенням металевих конструкцій. Для досвіду були використані три окремі точки доступу, розставлені у випадкових місцях. Перші дві -Cisco AP350s. На першій було встановлено дві антени, друга не містила антени. Третя моделі Orinoco AP-1000 з антеною Lucent.

Збір даних

Першим завданням був збір значень залежності сили сигналу від дистанції, базуючись на даних, представлених драйвером бездротової карти. Для збору даних використовувалася програма iwspy, налаштована на певну MAC адресу:

```
# iwspy eth0 0b:0b:0b:0b:0b:0b
```

Послідовний виклик "iwspy eth0" буде повертати значення рівня сигналу пакетів, отриманих від даного передавача.

Тестуюча станція переміщається по території, вимірюючи потужність сигналу у випадкових точках. Для обробки представляється файл, що складається з двох колонок, в першій відстань від передавача, в другій рівень сигналу. Графічно значення показані на Рис. 3.3 - Рис. 3.5

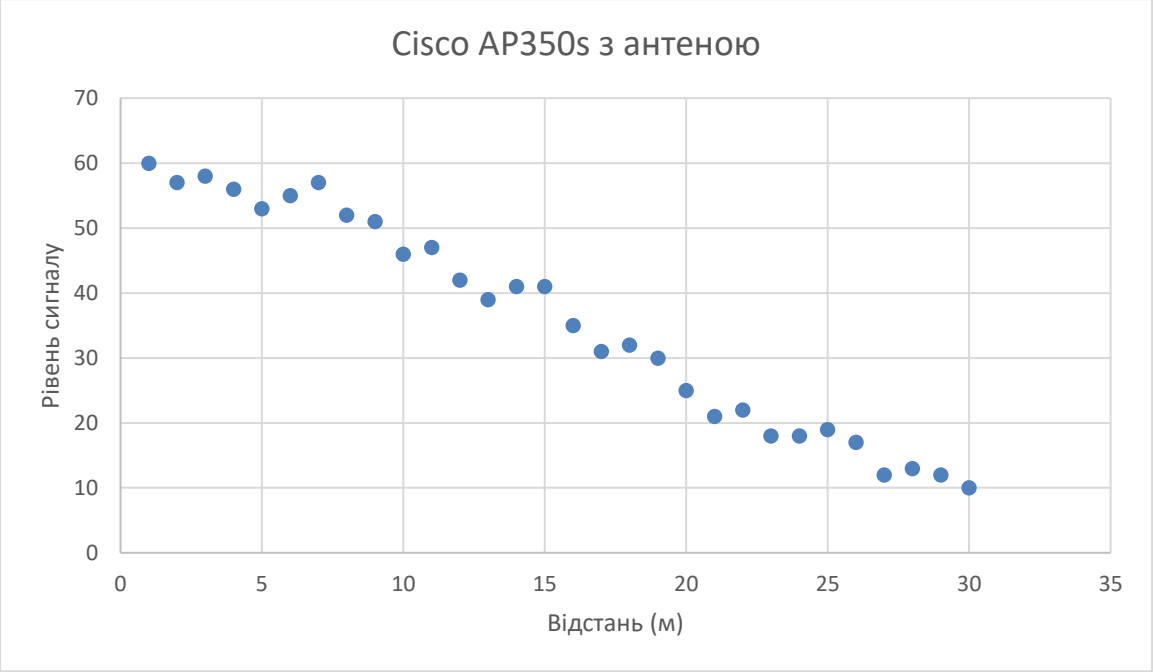


Рисунок 3.3 Cisco AP350s з антеною

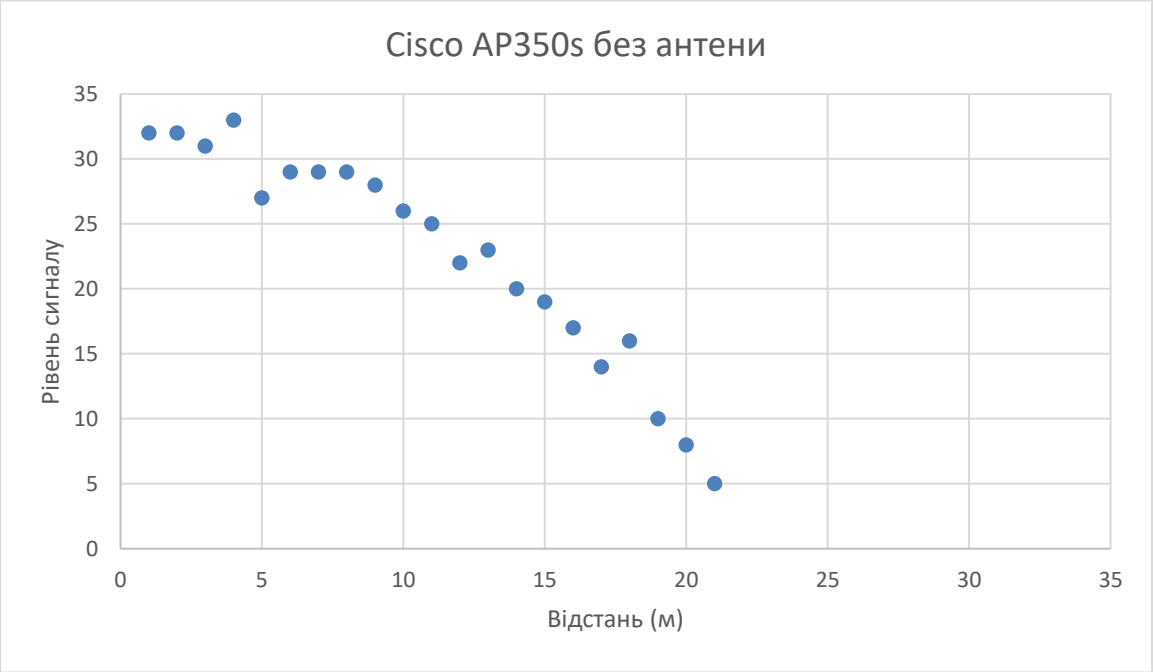


Рисунок 3.4 Cisco AP350s без антени

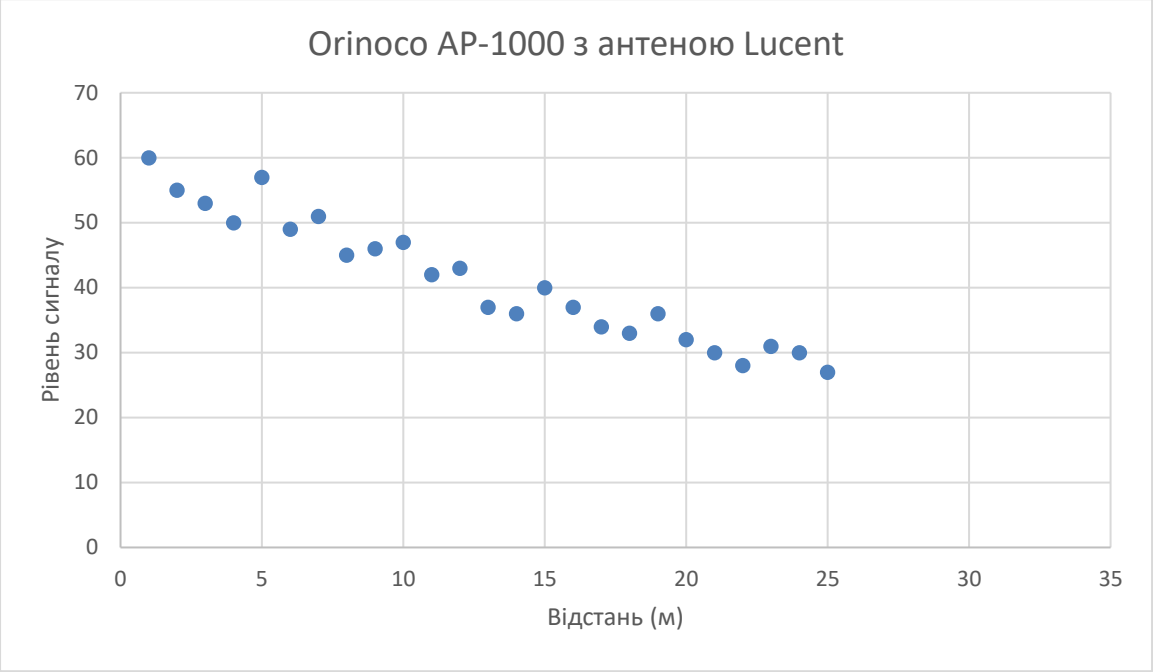


Рисунок 3.5 Orinoco AP-1000 з антеною Lucent

Знаходження залежності сили сигналу від дистанції

Наступним кроком необхідно визначити, чи можуть дані, отримані в ході попереднього експерименту, задовольняти співвідношенню, наведеним на початку глави.

Для цього необхідно спочатку перевести значення (RSSI - значення рівня прийнятого сигналу), отримані за допомогою утиліти iwspy, в Дб. Експерементально отримані наступні залежності:

$$P_{dBm} = 1{,}205P_{RSSI} - 101{,}07$$

$$P_{RSSI} = 0{,}83P_{dBm} + 83{,}891$$

Де: PdBm - значення рівня сигналу в ДБ, PRSSI - значення, отримане за допомогою утиліти iwspy.

Якщо значення видаються в нормалізованому вигляді (дана опція встановлюється в драйвері бездротової карти), рівняння набувають вигляду:

$$P_{dBm} = 0{,}62N_{RSSI} - 101{,}07$$

$$N_{RSSI} = 1{,}66P_{dBm} + 167{,}782$$

В даний час iwspy ioctl для Linux повертає не нормалізовані значення (проте, клієнт Cisco для ОС Windows повертає нормалізовані значення).

Наступним етапом є побудова функції апроксимації кривих, в яку включені наведені вище залежності. В якості базису використовується рівняння, що враховує як загасання при поширенні радіохвиль в приміщенні, так і відображення, рефракцію і інтерференцію.

В результаті експериментів і досліджень було отримано наступне співвідношення для поширення радіосигналу в будівлі на частоті 2,4 ГГц.

Таким чином, на 10 метрів втрати складуть приблизно 75 Дб на 100 метрів 110 Дб. Очікувана похибка перебувати в діапазоні 13 Дб.

Всі невідомі константи, в тому числі значення «40», яке отримано в результаті експериментів, буде об'єднано в одну константу C, де C - невідома константа, що визначає вихідну потужність з урахуванням впливу загасань, конфігурації антени та інших факторів.

$$R_d = C - 35log_{10}D$$

За допомогою співвідношення, наведеного нижче, проведемо перетворення значення в не нормоване (для відповідності значень вихідним даними утиліти iwspy під Linux):

$$P_{RSSI} = 0{,}83(C - 35log_{10}D) + 83{,}891$$

Створимо програму, для побудови апроксимаційної функції в середовищі Gnuplot, використовуючи дані, показані на Рис. 3.6.1 - Рис. 3.6.3

```
set view ,,.5
sstodbm(ss) = ss * 1.205 - 101.07
dbmtoss(dbm) = dbm * .83-+ 83.891
f(x) = dbmtoss { a - 35 * (log(x)/log(10)) )
```

```
fit f(x) "ld-distance-data/cisco-chan6-antenna.txt" via a
plot [0:25] [0:62] "ld-distance-data/cisco-chan6-antenna.txt", f(x)
pause -1 "Hit return to continue"
fit f(x) "ld-distance-data/cisco-chan6-no-antenna.txt" via a
plot [0:25] [0:62] "ld-distance-data/cisco-chan6-no-antenna.txt", f(x)
pause -1 "Hit return to continue"
fit f(x) "ld-distance-data/orinoco-chan3-antenna.txt" via a
plot [0:25] [0:62] "ld-distance-data/orinoco-chan3-antenna.txt", f(x)
pause -1 "Hit return to continue"
```

Отримана крива апроксимації для кожного з випадків.

Шляхи підвищення ефективності пошуку

1.Підвищення достовірності результатів, незалежність від числа каналів. В ідеалі, пошукова станція повинна сканувати всі частоти по всьому спектру одночасно;

2.Отримане співвідношення між значеннями рівня сигналу в Дб і значенням, її обчислене драйвером карти Cisco, не завжди точно, і, в деяких ситуаціях, може бути не лінійно;

3.Включення до складу комплексу GPS навігації може значно поліпшити результати і спростити збір даних;

4.Залучення як мінімум 3-х пошукових станцій значно поліпшить результати;

5.Застосування спеціального аналізатора пакетів, спеціально розрахованого на роботу з бездротовою мережею;

6.Розробка протоколу, що дозволяє пошуковим станціям обмінюватися даними і здійснювати спільний моніторинг;

7.Розробка вдосконаленого алгоритму, що дозволяє зменшити вплив похибок при вимірюванні відстані;

8.Створення математичної моделі ландшафту з урахуванням можливостей загасання сигналу;

9.Збір бази даних, що описує очікувану потужність передавачів різних виробників, в тому числі із застосуванням антени, так і без, що дозволить більш точно локалізувати джерело сигналу;

10. Комбінувати даний підхід з методами, в яких використовуються спрямовані антени.

ВИСНОВКИ ДО РОЗДІЛУ 3

1. Аналіз результатів показав високу ефективність застосування даного комплексу заходів для запобігання можливості атаки на бездротову мережу;

2. Виявлені найбільш ймовірні причини виникнення помилок при обчисленні координат:

2.1. Загасання сигналу від антени передавача було велике. На шляху сигналу розташовувалися перешкоди;

2.2. Передавач розташовувався в середині приміщення, отже не вдалося зібрати достовірну інформацію про загасання сигналу на граничних відстанях;

2.3. Передавач розташовувався в приміщенні з великою кількістю металевих предметів, що додатково послаблювало і экранировало сигнал в певних напрямках.

3.До основних обмежень запропонованого методу відносяться:

3.1 при використанні даної технології неможливо визначити місце розташування неактивної станції;

3.2 Драйвер і мережева карта Cisco обмежені в можливості . сканування довільного трафіку, таким чином деяка кількість корисних даних могла бути загублена в ході експерименту;

4. Карта Cisco не може сканувати кілька каналів одночасно. При виникненні сигналу: від неавторизованої станції, всі карти, задіяні для захисту мережі повинні преостановить сканування і переключитися на цей канал, з метою найбільш повного збору інформації. Показано застосування вдосконаленої системи безпеки на практиці.

5. Якщо застосовується більш ніж одна станція, всі вони повинні володіти ідентичними версіями мережевих карт (в тому числі антен)і драйверів;

6. Збільшення кількості станцій, що беруть участь в пошуку збільшує шанс на вдале позиціонування;

7. Пошукові станції, у разі, якщо вони розташовані стаціонарно, повинні бути розташовані найбільш оптимально: на максимально можливій відстані один від одного, на відкритому просторі, максимально, виключаючи можливі ослаблення сигналу від перешкод або перешкод, але в той же час, щоб вони могли приймати сигнал з будь-якого місця охоронюваної зони;

8. Слід встановити активно скануючу мережа станцію, яка в разі появи неавторизованого передавача буде посилати запити, що вимагають відповідей, за якими буде можливо визначити потужність сигналу;

9. Для пошукових станцій необхідні високочутливі антени;

10. У разі мобільного неавторизованого пристрою дана технологія не зможе принести належних результатів;

РОЗДІЛ 4. МАРКЕТИНГОВИЙ АНАЛІЗ СТАРТАП-ПРОЕКТУ

4.1 ОПИС ІДЕЇ ПРОЕКТУ

Таблиця 4.1. Опис ідеї стартап-проекту

Зміст ідеї	Напрямки застосування	Вигоди для користучача
вирішення задачі захисту інформації в радіоканалах мобільних робототехнічних комплексів, шляхом застосування комплексних заходів для захисту від можливих атак спрямованих на перехоплення і підміну переданих даних	забезпечення необхідної умови захищеності інформації	значно знижена ймовірність атак на інформацію в радіоканалах. Достовірність наукових положень дисертації підтверджена: виконаними експериментальними дослідженнями, практичною реалізацією системи захисту даних у радіоканалі МРК та результатами впровадження.

Економічні характеристики — вартість обслуговування, експлуатації, ремонт, ціна.

Технічні характеристики продукту стосуються напрямку використання товару - розміри, кількість елементів, функції, характеристики матеріалу.

Таблиця 4.2. Опис ідеї стартап-проекту

№	Техніко-економічні характеритики ідеї	Продукція конкурентів				W (слабка сторона)	N (нейтральна сторона)	S (сильна сторона)
		Мій	Потенційний	Конкурент 2	Конкурент 3			
1	Собівартість реалізованої продукції (товарів, робіт, послуг), $ за од. продукції(лист із спрогнозованими даними)	35	60	50	50	-	-	+
2	Чистий прибуток	25	20	10	10	-	-	+

4.2 ТЕХНОЛОГІЧНИЙ АУДИТ ІДЕЇ ПРОЕКТУ

Таблиця 4.3. Технологічна здійсненність ідеї проекту

№	Ідея проекту	Технології її реалізації	Наявність технологій	Доступність технологій
1	Система аутентифікації	алгоритмі SPEKE	+	+
2	Система сканування	карта Cisco	+	-
Обрана технологія реалізації ідеї проекту:1				

Висновок: технологічна реалізація продукту – можлива, вибрана технологія №1.

4.3 АНАЛІЗ РИНКОВИХ МОЖЛИВОСТЕЙ ЗАПУСКУ СТАРТАП-ПРОЕТКУ

Таблиця 4.4. Попередня характеристика потенційного ринку

№	Показники стану ринку	Характеристика
1	Кількість головних гравців, од	1
2	Загальний обсяг продаж, грн./ум.од	1
3	Динаміка ринку	зростає
4	Наявність обмежень для входу	В бездротовій мережі пред'являються підвищені вимоги з безпеки. Необхідно використовувати криптографічно стійкі алгоритми
5	Специфічні вимоги до стандартизації та сертифікації	Стандартизація IEEE 802.11
6	Середня норма рентабельності в галузі або по ринку, %	Рп = П / ТО = Прибуток / Товарообіг = 250$ / 25$ = 10%

Висновок: враховуючи кількість головних гравців по ринку, зростаючу динаміку ринку, невелику кількість конкурентів та середню норму рентабельності можна зробити висновок, що на даний момент, ринок для входження стартап-продукту є привабливим.

Таблиця 4.5. Характеристика потенційних клієнтів стартап-проекту

№	Потреба, що формує ринок	Цільова аудиторія	Відмінності у поведінці цільових груп клієнтів	Вимоги споживачів до товару
1	Недоліки в області захисту даних, використання	Будь-які користувачі, зацікавлені в підвищенні захисту свої	Відсутні.	Максимально точні значення пошуку активних

	стандартних методів	данних при передачі радіотехнологією		станцій-порушників.

Таблиця 4.6. Фактори загроз

№	Фактор	Зміст загрози	Можлива реакція компанії
1	Конкуренти	Наявність конкурентів котрі надають схожі рішення	Зменшення ціни на поставлену послугу; Розробка унікальних характеристик товару; Надання ліцензій на обслуговування
2	Кошти на розробку та підтримку продукту	Закінчення грошей та недостатнє фінансування	Залучення додаткових інвесторів, мотивація роботи на перспективу; Ітеративна розробка продукту задля покрокового виведення продукту на ринок та отримання відповіді користувачів
3	Вихід аналогу	Вихід аналогу даного товару може призвести до знецінення та безідейності даного товару	Вихід товару на ринок в коротші строки з не повною, але достатньою, функціональністю для зацікавлення усіх цільових аудиторій; Проведення рекламної компанії

Таблиця 4.7. Фактори можливостей

№	Фактор	Зміст можливості	Можлива реакція компанії
1	Новий продукт	Вихід на ринок, Зменшення монополії,	Розробка нової функціональності;

		Надання нових рішень у сфері	Вихід нової продукції на ринок; Надання різноманітних типів ліцензій в залежності від потреб користувача \ замовника.
2	Вихід аналогу	Надати продукт з певними характеристиками та можливостями що відсутні у компаній конкурентів	Аналіз ринку та користувачів задля задоволення їх потреб та надання функціональності у найкоротші строки за ціну, котра є дешевшою ніж у продуктів-замінників.
3	Зворотній зв’язок від користувачів	Можливість отримання необхідної інформації для вдосконалення продукту	Наявність вхідних даних та реакція на них з боку команди розробників задля задоволення потреб та бажань кінцевих користувачів системи кешування даних.
4	Грошова винагорода за рекламу	При достатньому попиту на систему кешування даних можлива комерціалізація продукту на основі реклами задля отримання грошової винагороди для подальшого розвиту продукту та оплати заробітної плати працівникам	Точкова комерціалізація продукту; Введення реклами; Ведення додаткових коштів у проект задля його подальшого розвитку.

Таблиця 4.9. Ступеневий аналіз конкуренції на ринку

№	Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)
1	Тип конкуренції: монополістична	Товар від кожної компанії на ринку, являється недосконалим замінником товару, реалізованого іншими фірмами; на ринку є умови для входу та виходу; ціна корелює між суперниками.	Розробка продукту з характеристиками, які покривають сфери вживання що не покривають інші товари-замінники; кореляція цін у відповідності до товарів замінників; різни типи ліцензій.
2	Рівень конкурентної боротьби: світовий	Всі продукти замінники розроблялись інтернаціональними командами з різних куточків світу, продукти не належать до певної держави, а належать команді розробників	Вихід на ринок збуту продукту з клієнто-необхідною функціональністю; налагодження маркетингу на основних Інтернет ресурсах задля охоплення великої кількості потенційних користувачів; надання бета-версій продукту.
3	Галузева ознака: внутрішньогалузева	Даний тип продукту може використовуватися тільки у сфері розробки ІТ додатків \ продуктів.	Надання зручного, інтуїтивно зрозумілого інтерфейсу; підтримка всім відомих методів взаємодії з середовищем розробки; наявність документації та онлайн підтримки.
4	Конкуренція за видами товарів: товарно-видова	Дана конкуренція – конкуренція між товарами одного виду.	Впровадження функціональності яка відсутня у товарів-замінників; спрощення інтерфейсів; надання підтримки.

5	Характер конкурентних переваг: цінова та не цінова	Цінові переваги – точкова комерціалізація; не цінова – надання функціональності, що відсутня у товарах-замінниках.	Надання платних ліцензій лише на критично важливу функціональність для клієнта з певним строком підтримки, що зазначена у відповідній ліцензії; впровадження унікальної функціональності.
6	За інтенсивністю: марочна	Наявність унікального знаку що відрізняє даний продукт від продуктів-замінників	Впровадження власної назви та власного знаку.

Таблиця 4.10. Аналіз конкуренції в галузі за М. Портером

Складові аналізу	Прямі конкуренти в галузі	Потенційні конкуренти	Постачальники	Клієнти	Товари замінники
	Відсутні	Підприємці-новачки	Ринкова влада	Будь-який користувач бездротових мереж	Системи, які надають більш точні результати за нижчими цінами
Висновки	На момент входу на ринок буде час знайти покупців(налагодити канали збуту), закріпити позиції на ринку, монополізувати ринок саме для цього виду товару на певний час, підвищити точність захисту за рахуннок оновлення	Загроза появи нових конкурентів усередині галузі, проте у конкурентів може бути відсутній досвід у сфері продажу захисту даних, не налагоджені канали збуту, відсутні високі показники прогнозів, що є ключовим аспектом при виборі продавця		Чим більше клієнтів, тим більший попит	Загроза втрати керівної позиції на ринку

Проаналізувавши можливості роботи на ринку з огляду на конкурентну ситуацію можна зробити висновок: оскільки кожний з існуючих продуктів не впливає у великій мірі на поточну ситуацію на ринку в цілому, кожний з існуючих продуктів має свою специфічну сферу використання та свої позитивні та негативні сторони щодо рішення певних типів задач, то робота та вихід на даний ринок є можливою і реалізованою задачею.

Для виходу на ринок продукт повинен мати функціонал що відсутній у продуктів-аналогів, повинен задовольняти потреби користувачів, мати необхідний та достатній функціонал з конфігурування, підтримку зі сторони розробників та можливість розробки спеціального функціоналу за відповідною ліцензією.

Таблиця 4.11. Обґрунтування факторів конкурентоспроможності

№	Фактор конкурентоспроможності	Обґрунтування
1	Частка ринку	Враховуючи той факт, що тип родового середовища в галузі – консолідований ринок, тобто існує група компаній, які контролюють разом понад 40% ринку, а також те, що інтенсивність суперництва між діючими конкурентами при низьких темпах зростання ринку є однією з головних сил, які діють на конкуренцію в галузі, одним з найважливіших факторів конкурентоспроможності виступає частка ринку, яку займає виробник. Чим більша частка ринку, тим більшими ринковими можливостями володіє виробник
2	Ціна	Держава вибиратиме тих підприємців, у яких товар(в даному випадку спрогнозовані

		значення) коштує мінімально, а результати дає максимальні, тому ціна так само, як і якість є одним із засобів ведення конкурентної бороти.
3	Асортимент	За рахунок розширення асортименту(захисту даних) можна вести конкуренту боротьбу.
4	Доступ до каналів розподілу	Головний канал через який відбуватиметься розподіл – це держава. Товар продаватиметься державі, опісля держава розповсюджуватиме його серед учасників ринкових відносин.
5	Торговий маркетинг	
6	Рівень диференціації ТМ	Державі надається список унікальних цінностей захисту даних.
7	Репутація виробника	Репутація виробника важлива при виході на ринок з новими товарами, або при виході на нові сегменти, що полегшує позитивне сприйняття новинок
8	Рівень лояльності до бренду	Чим вище рівень лояльності, тим більше компанія має прихильних, а значить постійних споживачів.
9	Унікальність позиціонування	На даний момент на ринку буде монополістична конкуренція.
10	Маркетинговий бюджет	Від розміру маркетингового бюджету залежить здатність здійснювати маркетингову стратегію підприємства. Маркетингові заходи мають забезпечувати інші конкурентні переваги такі, як рівень диференціації, лояльності, репутація виробника, дистрибуція та просування в торгових точках.

Таблиця 4.12. Порівняльний аналіз сильних та слабких сторін моделі захисту інформації при передачі радіотехнологією

№	Фактор конкурентоспроможності	Бали 1-20	Рейтинг товарів-конкурентів у порівнянні з запропонованим						
			-3	-2	-1	0	+1	+2	+3
1	Частка ринку	2	-	-	-	-	-	+	-
2	Ціна	-2	-	+	-	-	-	-	-
3	Асортимент	0	-	-	-	+	-	-	-
4	Доступ до каналів розподілу	-1	-	-	+	-	-	-	-
5	Торговий маркетинг	0	-	-	-	+	-	-	-
6	Рівень диференціації ТМ	0	-	-	-	+	-	-	-
7	Репутація виробника	3	-	-	-	-	-	-	+
8	Рівень лояльності до бренду	0	-	-	-	+	-	-	-
9	Унікальність позиціонування	-3	+	-	-	-	-	-	-
10	Маркетинговий бюджет	1	-	-	-	-	+	-	-

Таблиця 4.13. SWOT аналіз стартап-проекту

Сильні сторони (S):	Слабкі сторони (W):
– висока точність виявлення станції-порушника; – можливість регулярно постачати нову інформаціюпро станцію-порушника; – можливість постійного покращення точності значень за рахунок навчання мережі;	– захист с точністю 90-95%; – необхідний постійний розвиток системи і покращення результатів.

Можливості (О):	Загрози (Т):
– підвищити відсоток захисту системи.	– конкуренти, які надаватимуть результати із такою ж точністю швидше.

Таблиця 4.14. Альтернативи ринкового впровадження стартап-проекту

№	Альтернатива (орієнтовний комплекс заходів) ринкової поведінки	Ймовірність отримання ресурсів	Строки реалізації
1	Безкоштовне надання певного функціоналу у користування споживачам на обмежений термін	Головний ресурс – люди, даний ресурс - наявний	1 місяць
2	Реклама	Залучення власних коштів для реклами товару	1-2 місяці
3	Написання статей та опис товару на відомих ресурсах	Головний ресурс – час, даний ресурс - наявний	2 тижні
4	Презентація товару на хакатонах й інших ІТ заходах	Ресурс – час та гроші для участі, наявні	2-3 місяці

4.4 РОЗРОБЛЕННЯ РИНКОВОЇ СТРАТЕГІЇ ПРОЕКТУ

Таблиця 4.15. Вибір цільових груп потенційних споживачів

№	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи (сегменту)	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
1	Кожен учасник бездротової мережі	Кожен підприємець, який бажає надійно захистити свою компанію. Спекулянти будуть упиратися.	90% сегменту ринку	Інтенсивність буде значною, збільшуватиметься з часом	Аналоги існують, важливим етапом буде налагодження зв’язків із державою для отримання каналу збуту
Які цільові групи обрано: групу 1 (весь ринок)					

Відповідно до проведеного аналізу можна зробити висновок, що підходящою цільовою групою для розповсюдження даного програмного продукту є будь-яка бездротова мережа, учасники якої бажають покращити захист при передачі даних. Відповідно до стратегії охоплення ринку збуту товару обрано стратегію масового маркетингу, так як продукт(спрогнозовані значення) надається стандартизований продукт з можливістю розширення функціональності за домовленістю (відповідно до ліцензії).

Таблиця 4.16. Визначення базової стратегії розвитку

Обрана альтернатива розвитку проекту	Стратегія охоплення ринку	Ключові конкурентоспроможні позиції відповідно до обраної альтернативи	Базова стратегія розвитку
Надання функціональності що відсутня у товарів-замінників, підтримка клієнтів	Проведення реклами, освітлення унікальної функціональності через інтернет ресурси та інші канали, контакт напряму з споживачами; формування лояльності і прихильності споживачів	Зниження ступеню замінності товару; Прихильність клієнтів; Відмітні властивості товару; Відмітні характеристики товару;	Стратегія диференціації

Таблиця 4.17. Визначення базової стратегії конкурентної поведінки

Чи є проект «першопрохідцем» на ринку	Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?	Чи буде компанія копіювати основні характеристики товару конкурента, які?	Стратегія конкурентної поведінки
Ні, оскільки є товари-заміннники, але дані товари замінники не мають деякого необхідної якості	Так, ціль компанії знайти нових споживачів та, частково, забрати існуючих у конкурентів задля задоволення потреб останніх	Компанія частково копіює характеристики товару конкурента, основна ціль компанії розробка покращеної якості, з підтримкою основного функціоналу конкурентів	Стратегія заняття конкурентної ніші

Таблиця 4.18. Визначення стратегії позиціонування

№	Вимоги до товару цільової аудиторії	Базова стратегія розвитку	Ключові конкурентоспроможні позиції власного стартап-проекту	Вибір асоціацій, які мають сформувати комплексну позицію власного проекту
1	Точність спрогнозованих даних	Наступальна або атакуюча стратегія	Інноваційна і технологічна	
2	Доступна ціна	Наступальна або атакуюча стратегія	Ресурсна позиція	
3	Регулярні часті поставки значень	Наступальна або атакуюча стратегія	Організаційна позиція	

Відповідно до проведеного аналізу можна зробити висновок, що стартап-компанія вибирає як базову стратегію розвитку – стратегію диференціації, як базову стратегію конкурентної поведінки – стратегію заняття конкурентної ніші.

4.5 РОЗРОБЛЕННЯ МАРКЕТИНГОВОЇ ПРОГРАМИ СТАРТАП-ПРОЕКТУ

Таблиця 4.19. Визначення ключових переваг концепції потенційного товару

№	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити)
1	Надійний захист при передачі даних радіотехнологією	Підвищення якості захисту інформації	Підвищення ефективності якості захисту інформації при предачі радіотехнологією, доступність для кожного учасника

Таблиця 4.20. Опис трьох рівнів моделі товару

Рівні товару	Сутність та складові		
1. Товар за задумом	Отримання максимально точних результатів по кількості знежкоджених атак на максимально довгий період		
2. Товар у реальному виконанні	Властивості/характеристики	М/Нм	Вр/Тх/Тл/Е/Ор
	Зовнішній вигляд(значення у текстовому форматі)	Нм	Вр/Тх/Тл/Е
	Точність	Нм	Вр/Тх/Тл
	Кількість спрогнозованих значень	М	Вр/Тх/Тл
	Термін зберігання	М	Вр/Тл
	Пакування: дані упаковані в файл формату CSV		
3. Товар із підкріпленням	До продажу: наявна повна документація		
	Після продажу: додаткова підтримка спеціалістів налаштування, підтримка з боку розробника		
За рахунок оформлення патенту потенційний товар буде захищено від копіювання			

В/Нв – відчутні/невідчутні; М/Нм – монотонні/немонотонні; Пр/Нпр – параметричні/непараметичні; Вр/Тх/Тл/Е/Ор – вартісні/ технічні/ технологічні/ ергономічні/ органолептичні; О/К/С – обов'язкові/ кількісні/ сюрпризні

Таблиця 4.21. Визначення меж встановлення ціни

Рівень цін на товари-замінники	Рівень цін на товари-аналоги	Рівень доходів цільової групи споживачів	Верхня та нижня межі встановлення ціни на товар/послугу
60-100$	20-60$	Від середнього до високого	10 – 100$

Таблиця 4.22. Формування системи збуту

Специфіка закупівельної поведінки цільових клієнтів	Функції збуту, які має виконувати постачальник товару	Глибина каналу збуту	Оптимальна система збуту
Специфіка залежить в регіону користувачів	Надання надання надійного захисту та звіту по захисту, деактивованих станцій-порушників, кількості атак	Канал першого, другого рівня	Купівля ліцезійного продукту, поширення через інтернет, постачання ПЗ разом з обладнанням

Таблиця 4.23. Концепція маркетингових комунікацій

№	Специфіка поведінки цільових клієнтів	Канали комунікацій, якими користуються цільові клієнти	Ключові позиції, обрані для позиціонування	Завдання рекламного повідомлення	Концепція рекламного звернення

1	Недовіра до нової системи захисту, так як існують аналоги	Будь-які інтернет засоби зв’язку(пошта, чати, програмні застосунки для дзвінків(skype, viber)), засоби зв’язку по телефону	Реклама, паблік форуми, стимулювання збуту, особисті продажу	Викликати довіру у потенційного клієнту	Приклад захисту даних на тестовому середовищі, щоб одразу на прикладі було видно результат, який можна швидко перевірити

Як результат було створено ринкову (маркетингову) програму, що включає в себе визначення ключових переваг концепції потенційного товару, опис моделі товару, визначення меж встановлення ціни, формування системи збуту та концепцію маркетингових комунікацій.

ВИСНОВКИ ПО РОЗДІЛУ 4

В четвертому розділі описано стратегії та підходи з розроблення стартап-проекту, визначено наявність попиту, динаміку та рентабельність роботи ринку, як висновок було вказано що існує можливість ринкової комерціалізації проекту.

Розглянувши потенційні групи клієнтів, бар’єри входження, стан конкуренції та конкурентоспроможність проекту було встановлено що проект є перспективним. Розглянуто та вибрано альтернативу впровадження стартап-проекту та доведено доцільність подальшої імплементації проекту.

ВИСНОВКИ

Мета, сформульована в магістерській роботі, по проведенню аналізу безпеки бездротових мереж, виділення методів їх захисту та створення моделі захисту бездротових мереж виконана.

1. Проведено дослідження особливостей роботи стандартного протоколу потокового шифрування WEP. Для кожного з видів атак розроблено методи протидії, що дозволяють підвищити ступінь захисту даних в радіоканалі.
2. Розроблено система аутентифікації, заснована на алгоритмі SPEKE. Проведено дослідження з точки зору захисту інформації, проаналізовано механізми виникнення атак, створено методи протидії. Розроблено систему яка є заміною стандартним засобам аутентифікації протоколу 802.11, що не володіє достатнім рівнем безпеки.
3. На основі алгоритму SPEKE створено механізм захищеного обміну ключами сесії, відсутній у стандартній системі безпеки. Можливість зміни ключа сесії дозволить знизити ймовірність успішних атак на інформацію, зашифровану за допомогою алгоритму потокового шифрування WEP.
4. Створено вдосконалену систему захисту інформації, переданої у радіоканалі 802.11, що дозволяє значно підвищити рівень захисту інформації, у порівнянні зі стандартною системою, за рахунок застосування комплексу криптографічно стійких засобів і методів шифрування, аутентифікації і обміну ключами.
5. Розроблено технологію, що дозволяє використовувати особливості протоколу 802.11 для локалізації станції-порушника, розміщеної у зоні роботи бездротової мережі. Створено методи підвищення ефективності роботи системи пошуку активних станцій-порушників. Це дозволить значно знизити ймовірність атак на інформацію в радіоканалах. Достовірність наукових положень дисертації підтверджена: виконаними експериментальними

дослідженнями, практичною реалізацією системи захисту даних у радіоканалі та результатами впровадження.

Наведено методи збільшення швидкодії алгоритмів, засоби підвищення криптографічної стійкості системи захищеної аутентифікації;

На основі розроблених методів і засобів побудовано удосконалену систему безпеки для радіоканалу стандарту 802.11. Показано застосування вдосконаленої системи безпеки на практиці.

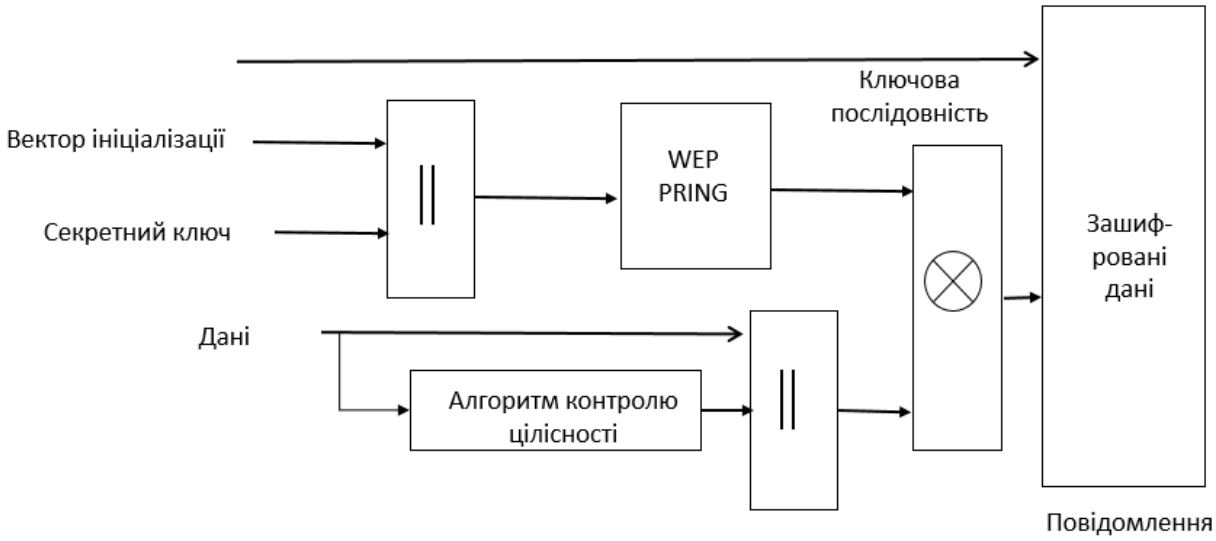
ПЕРЕЛІК ПОСИЛАНЬ

1. Анохин В.Л., Батанов А.Ф., Гамазов Н.И. Принципы автоматизации работ, выполняемых в экстремальных условиях робототехническими комплексами // Вестник МГТУ. Сер. Приборостроение. -1997. - №.2. - С. 75-81.
2. Вильям С. Криптография и защита сетей: принципы и практика, 2-е изд.- М.: Вильяме, 2001. - С. 672.
3. Воротников С. А., Михайлов Б. Б., Ющенко А.С. Адаптивная робототехническая система с интеллектуальной сенсорикой // Вестник МГТУ. Сер. Машиностроение. - 1995. - №.3. - С. 55 -58.
4. Джерело: Вихорев С., Кобцев Р. Як визначити джерела загроз.//Відкрита система. – 2002. - №07-08.С. 43.
5. Дружинин В.В., Конторов Д.С, Конторов М.Д. Введение в теориюконфликта. - М.: Радио и свіязь, 1989. - 288 с.
6. Королев В.И. Морозова Е.В. Методы оценки качества защиты информации при ее автоматизированной обработке // Безопасность информационных технологий. - 1995. - № 2. - 215 с.
7. Партыка Т. Л. ,Попов И. И. Информационная безопасность. - М: Форум - Инфра, 2002. - С. 368.
8. Поспелов Д.А. Неметкие множества в моделях управления и искусственногоинтеллекта. - М.: Наука, 1986. - 312 с.
9. Ротштсйн А.П. Интеллектуальные технологии идентификации. - Винница: «Универсум-Винница», 1999. - 320 с.
10. Успенский А. Ю. Операционные системы реального времени // Компью-Лог. - 2001. - №3. - С. 11 -17. - Успенский А. Ю. Применение интерфейса Photon в~системе управления робототехническим комплексом // Компью-Лог. - 2001.-№5.-С. 13-20.

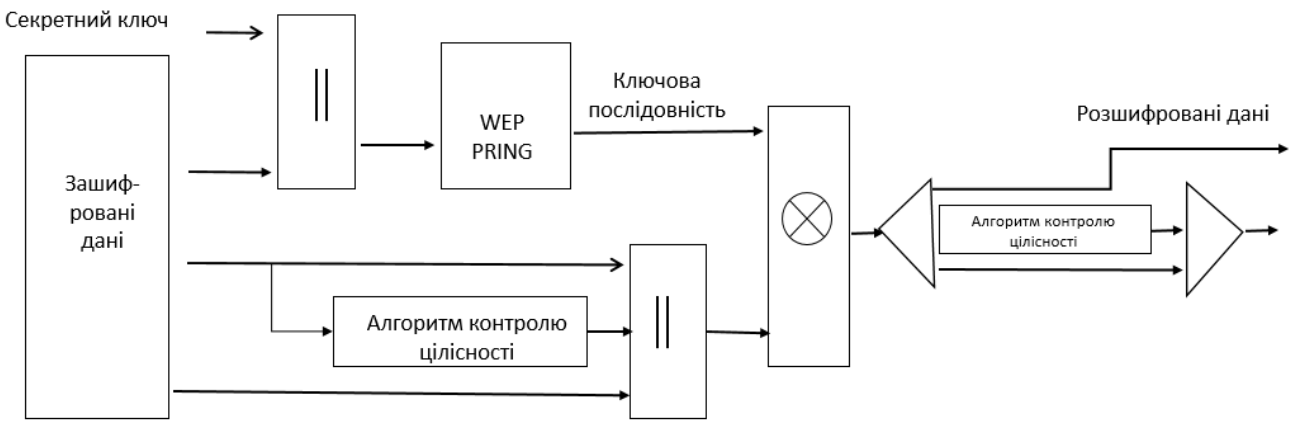
11. Успенский А.Ю. Исследование возможности и методы противодействия перехвату защищенной при помощи протокола WEP информации в радиоканале стандарта IEEE 802.11 // Студенческая научная весна - 2002. Сборник докладов студенческой научной конференции. - М.: 2002. - С. 89-91.
12. Успенский А.Ю., Иванов И.П. Анализ проблем защиты информации в радиоканалах стандарта IEEE 802.11 // Вестник МГТУ. Сер. Машиностроение. - 2002. - №. 4 - С. 102-108.
13. Ющенко А.С. Принципы интерактивного управления роботами // Робототехника: новый этап развития. - М.: Наука, 1993. - С. 129-139.
14. International Conference on Mobile Computing and Networking. -
15. ScarfoneKaren, PadgetteJohn. GuidetoBluetoothsecurity // NIST specialpublicationsep. 2008.
16. ScarfoneKaren, PadgetteJohn. GuidetoBluetoothsecurity // NIST specialpublicationsep. 2008.
17. Shim, Richard. How to Fill Wi-Fi's Security Holes, -Washington: ZDNet.-2001.-P. 21.
18. Steiner M., Tsudik G., Waidner M.. Refinement and Extension of Encrypted Key Exchange II Operating Systems Review.-1995 - 29, Iss. 3.-1995-22-30 p.
19. WEP Algorithm. II http://www.isaac.cs.berkeley.edu/isaac/wep

ДОДАТКИ

ДОДАТОК А



ДОДАТОК Б


Секретний ключ
Зашиф-
ровані
дані
WEP
PRING
Ключова
послідовність
Розшифровані дані
Алгоритм контролю
цілісності
Алгоритм контролю
цілісності

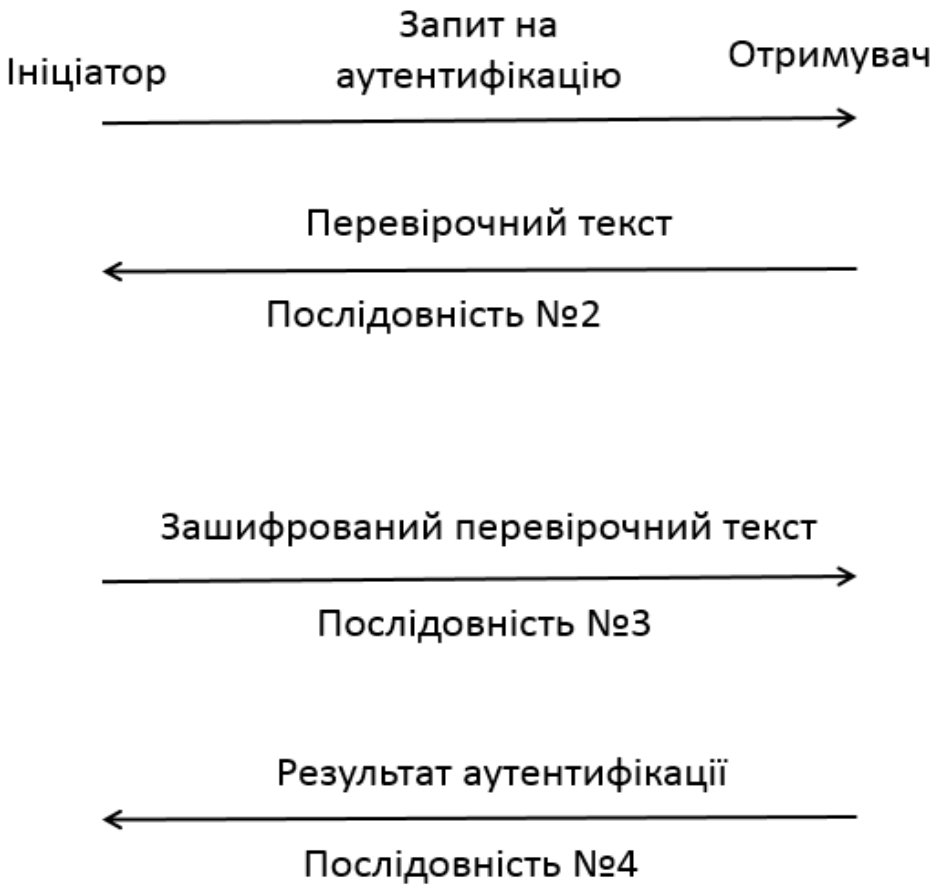
ДОДАТОК В


Основна підмережа
БД управління користувачами
Зовнішня мережа
Мережевий екран
WAN интерфейс
Внутрішня підмережа
Внутрішня мережа
WAN интерфейс
Міжмережевий екран безпроводної підмережі
Мережевий трафік
Точка доступу
Мобільний пристрій з інтерфейсом 802.11
Підмережа з бездротовим доступом (802.11)

ДОДАТОК Г

Розмір в октетах

ДОДАТОК Д


Ініціатор
Запит на аутентифікацію
Отримувач
Перевірочний текст
Послідовність №2
Зашифрований перевірочний текст
Послідовність №3
Результат аутентифікації
Послідовність №4